

21世纪高职高专规划教材

网络专业系列

计算机网络安全与管理

田庚林 田华 张少芳 编著





清华大学出版社

21 世纪高职高专规划教材·网络专业系列

计算机网络安全与管理

田庚林　田　华　张少芳　编著

清华大学出版社

内 容 简 介

本书介绍了计算机网络安全与管理技术，是面向高职高专计算机网络技术专业的教材。

本书以一个模拟网络工程为主线，分析网络工程中的安全管理需求，根据需求制定工程任务，按照任务介绍必备的知识，提出模拟工程中的解决方案，完成方案配置。

本书共分 7 章，内容包括模拟网络工程环境和模拟网络工程中的网络安全与管理需求分析、访问控制列表技术、局域网安全、网络地址转换技术、VPN 技术、防火墙技术、网络管理技术。

本书可以作为高职高专计算机网络技术及相关专业的教材，也可以作为网络工程技术人员和本科院校学生的参考书。

图书在版编目(CIP)数据

计算机网络安全与管理/田庚林，田华，张少芳编著. --北京：清华大学出版社，2010.3
(21 世纪高职高专规划教材. 网络专业系列)
ISBN 978-7-302-21818-0

Ⅰ. ①计…　Ⅱ. ①田…　②田…　③张…　Ⅲ. ①计算机网络—安全技术—高等学校：技术学校—教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2010)第 002689 号

责任编辑：刘　青
责任校对：刘　静
责任印制：

出版发行：清华大学出版社　　**地　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编**：100084
社 总 机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　销：全国新华书店
开　本：185×260　　**印　张**：17.5　　**字　数**：396 千字
版　次：2010 年 3 月第 1 版　　**印　次**：2010 年 3 月第1 次印刷
印　数：1～　000
定　价：　.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：033682-01

出版说明

高职高专教育是我国高等教育的重要组成部分，担负着为国家培养并输送生产、建设、管理、服务第一线高素质技术应用型人才的重任。

进入 21 世纪后，高职高专教育的改革和发展呈现出前所未有的发展势头，学生规模已占我国高等教育的半壁江山，成为我国高等教育的一支重要的生力军；办学理念上，“以就业为导向”成为高等职业教育改革与发展的主旋律。近两年来，教育部召开了三次产学研交流会，并启动四个专业的“国家技能型紧缺人才培养项目”，同时成立了 35 所示范性软件职业技术学院，进行两年制教学改革试点。这些举措都表明国家正在推动高职高专教育进行深层次的重大改革，向培养生产、服务第一线真正需要的应用型人才的方向发展。

为了顺应当前我国高职高专教育的发展形势，配合高职高专院校的教学改革和教材建设，进一步提高我国高职高专教育教材质量，在教育部的指导下，清华大学出版社组织出版了“21 世纪高职高专规划教材”。

为推动规划教材的建设，清华大学出版社组织并成立了“高职高专教育教材编审委员会”，旨在对清华版的全国性高职高专教材及教材选题进行评审，并向清华大学出版社推荐各院校办学特色鲜明、内容质量优秀的教材选题。教材选题由个人或各院校推荐，经编审委员会认真评审，最后由清华大学出版社出版。编审委员会的成员皆来自教改成效大、办学特色鲜明、师资实力强的高职高专院校、普通高校以及著名企业，教材的编写者和审定者都是从事高职高专教育第一线的骨干教师和专家。

编审委员会根据教育部最新文件和政策，规划教材体系，比如部分专业的两年制教材；“以就业为导向”，以“专业技能体系”为主，突出人才培养的实践性、应用性的原则，重新组织系列课程的教材结构，整合课程体系；按照教育部制定的“高职高专教育基础课程教学基本要求”，教材的基础理论以“必要、够用”为度，突出基础理论的应用和实践技能的培养。

本套规划教材的编写原则如下：

（1）根据岗位群设置教材系列，并成立系列教材编审委员会；

（2）由编审委员会规划教材、评审教材；

（3）重点课程进行立体化建设，突出案例式教学体系，加强实训教材的出版，完善教学服务体系；

（4）教材编写者由具有丰富的教学经验和多年实践经历的教师共同组成，建立“双师型”编者体系。

本套规划教材涵盖了公共基础课、计算机、电子信息、机械、经济管理以及服务等大类

的主要课程，包括专业基础课和专业主干课。目前已经规划的教材系列名称如下：

• 公共基础课

公共基础课系列

• 计算机类

计算机基础教育系列
计算机专业基础系列
计算机应用系列
网络专业系列
软件专业系列
电子商务专业系列

• 电子信息类

电子信息基础系列
微电子技术系列
通信技术系列
电气、自动化、应用电子技术系列

• 机械类

机械基础系列
机械设计与制造专业系列
数控技术系列
模具设计与制造系列

• 经济管理类

经济管理基础系列
市场营销系列
财务会计系列
企业管理系列
物流管理系列
财政金融系列
国际商务系列

• 服务类

艺术设计系列

本套规划教材的系列名称根据学科基础和岗位群方向设置，为各高职高专院校提供"自助餐"形式的教材。各院校在选择课程需要的教材时，专业课程可以根据岗位群选择系列；专业基础课程可以根据学科方向选择各类的基础课系列。例如，数控技术方向的专业课程可以在"数控技术系列"选择；数控技术专业需要的基础课程，属于计算机类课程的可以在"计算机基础教育系列"和"计算机应用系列"选择，属于机械类课程的可以在"机械基础系列"选择，属于电子信息类课程的可以在"电子信息基础系列"选择。依此类推。

为方便教师授课和学生学习，清华大学出版社正在建设本套教材的教学服务体系。本套教材先期选择重点课程和专业主干课程，进行立体化教材建设：加强多媒体教学课件或电子教案、素材库、学习盘、学习指导书等形式的制作和出版，开发网络课程。学校在选用教材时，可通过邮件或电话与我们联系获取相关服务，并通过与各院校的密切交流，使其日臻完善。

高职高专教育正处于新一轮改革时期，从专业设置、课程体系建设到教材编写，依然是新课题。希望各高职高专院校在教学实践中积极提出意见和建议，并向我们推荐优秀选题。反馈意见请发送到 E-mail：gzgz@tup.tsinghua.edu.cn。清华大学出版社将对已出版的教材不断地修订、完善，提高教材质量，完善教材服务体系，为我国的高职高专教育出版优秀的高质量的教材。

高职高专教育教材编审委员会

前　言

本书是一本面向高等职业教育的教材，是计算机网络技术专业系列教材之一。

在计算机网络技术专业建设中，从网络工程、网络管理岗位需求出发，我们将专业技能重点放在网络技术和网站技术两个方面。该专业系列教材中，将网络技术分为《计算机网络技术基础》、《计算机网络集成技术》、《计算机网络安全与管理》和《网络操作系统》4 门课程；网站技术主要包括《网页制作工具》、《网络数据库》、《动态网站技术》和《.NET 网站技术》4 门课程。本书主要介绍网络安全技术和基本的网络管理知识与基本管理技能。

本书以一个模拟的网络工程为主线，分析网络工程中的安全需求与管理任务；按照需求制定工程任务，按照任务需要介绍必备的知识，提出模拟工程中的解决方案，完成方案配置。本书内容既以工程需求为主，同时还照顾了知识体系的完整性与系统性。为了便于学生在实验室中对解决方案的配置、验证和测试，书中给出了一个网络安全与管理实训工程环境，实训环境可使用实际网络设备实现，也可使用模拟器软件实现。第 2 章至第 7 章的每章章后都有实训内容和实训指导，让学生根据在模拟工程实践中学到的知识技能完成实训项目，提高学生的动手能力与实践技能。

本书共分 7 章。第 1 章介绍模拟网络工程环境和模拟网络工程中的网络安全与管理需求分析；第 2 章介绍访问控制列表技术，根据工程任务安全需求分析，解决网络边界访问控制配置问题；第 3 章介绍局域网安全，根据工程任务安全需求分析，解决局域网中安全配置问题；第 4 章介绍网络地址转换技术，根据工程任务安全需求分析，解决网络中使用路由器进行内外网地址转换的配置问题；第 5 章介绍 VPN 技术，根据工程任务安全需求分析，解决利用 Internet 线路进行安全通信配置问题；第 6 章介绍防火墙技术，根据工程任务安全需求分析，解决网络边界安全中防火墙基本配置问题；第 7 章介绍网络管理技术，包括基本网络管理知识和常用的网络管理工具。附录中介绍了如何利用网络模拟器 GNS3 搭建模拟实训环境。本书中的网络设备都是以 Cisco 为例介绍的。

本书由田庚林主持编写，具体章节由田华、张少芳编写完成。其中，田庚林主要参与了内容的组织策划和统稿审定工作，第 3 章和第 4 章由张少芳编写完成，其余章节由田华编写完成。

由于计算机网络技术发展更新较快，作者水平有限，书中的不足之处望广大读者批评指正。作者 E-mail：tiangl163@163.com。

编　者

2009 年 12 月

目　录

第 1 章

计算机网络安全与管理任务分析

任何一个实际运行的计算机网络系统，特别是较大型的企业网络系统，为保证其安全、可靠地运行，必须建立相应的网络安全与管理方案，以减少各种潜在网络安全风险和网络性能瓶颈对信息系统正常运行的影响。本书以一个典型的跨地区公司网络系统为例，按照实际网络工程项目过程，先分析其中所需解决的网络安全与管理问题，然后介绍解决这些问题所需的知识和技术，最后给出这些问题的相应的解决方案。

1.1 公司网络环境

1.1.1 企业网络应用概况

某大型新兴产业公司为提高生产效率，拟新建联通各地分公司的计算机网络。该公司的总公司及其直属 3 个分支机构在 A 市，并在 B 市和 C 市分别设有一个子公司和两个分支机构。总公司和分公司主要负责产品的研发和生产，设有管理部门、研发部门、市场部门、售后服务部门和生产部门。各分支机构主要负责产品销售和售前、售后服务，设有市场部门、售后服务部门和管理部门。

公司所建网络将主要承载公司内部 OA、邮件、FTP、远程教育等系统和面向公众提供服务的电子商务网站系统。受业务发展、系统性能等诸多方面因素影响，以上网络应用系统设计在总公司、分公司分别设有网络应用及数据库服务器，而在分支机构只设网络终端。

1.1.2 企业网络拓扑结构

全公司的网络拓扑结构如图 1-1 所示。总公司与分公司利用电信专线互联，而为节约线路成本，总/分公司与其下属分支机构通过宽带线路接入本地 Internet 实现互联。

总公司局域网的网络拓扑结构按照网络应用需求分为核心、汇聚、接入 3 层，图 1-2 为总公司局域网的网络拓扑结构示意图。为了保证系统的安全可靠性，在各交换机上使用了双冗余线路设计。

分公司在局域网结构、链路冗余等方面与总公司类似。但分支机构 B-1、C-1 网络规模较大，而分支机构 B-2、C-2 网络规模较小，分支机构的网络拓扑结构如图 1-3 所示。

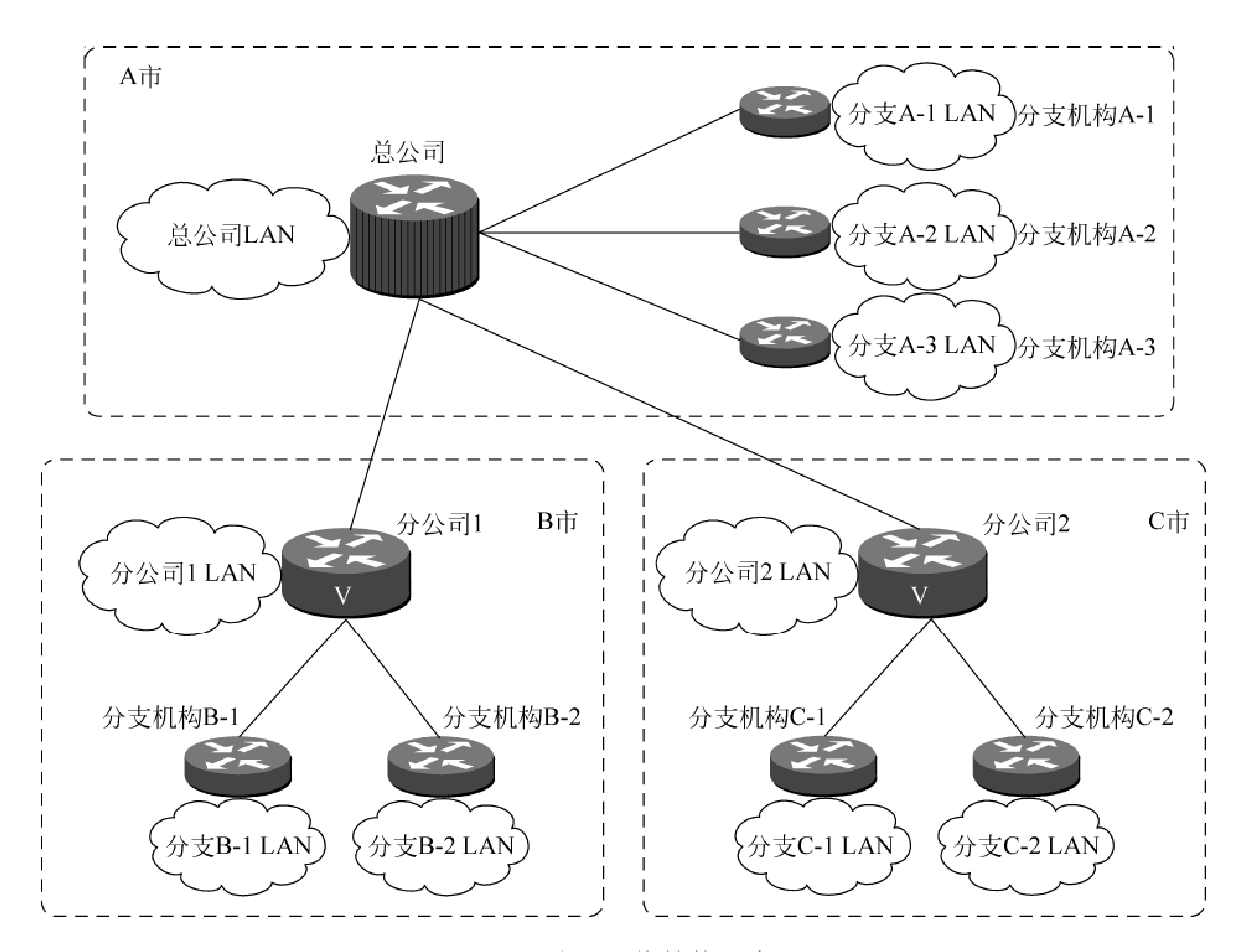


图 1-1 公司网络结构示意图

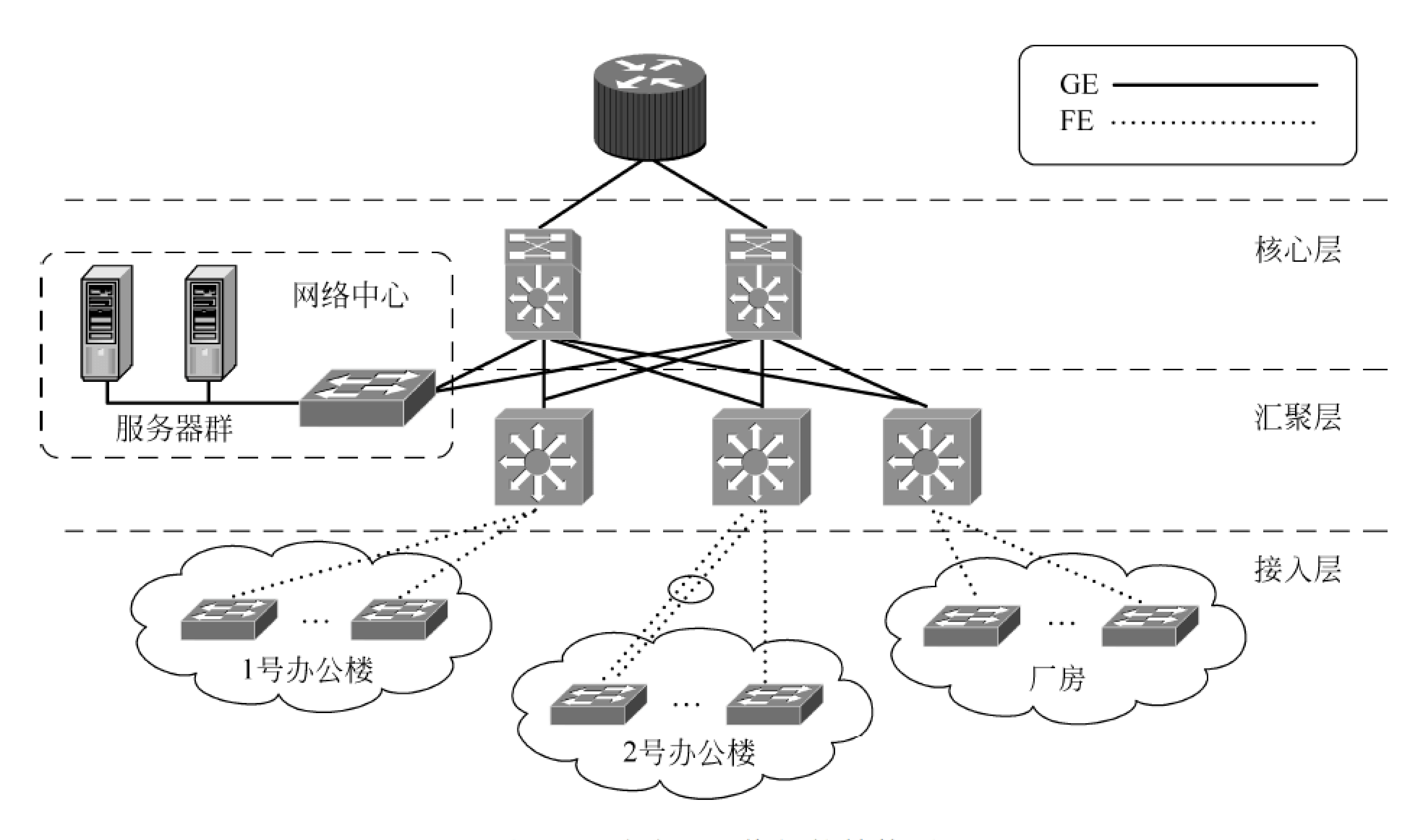


图 1-2 总公司网络拓扑结构图

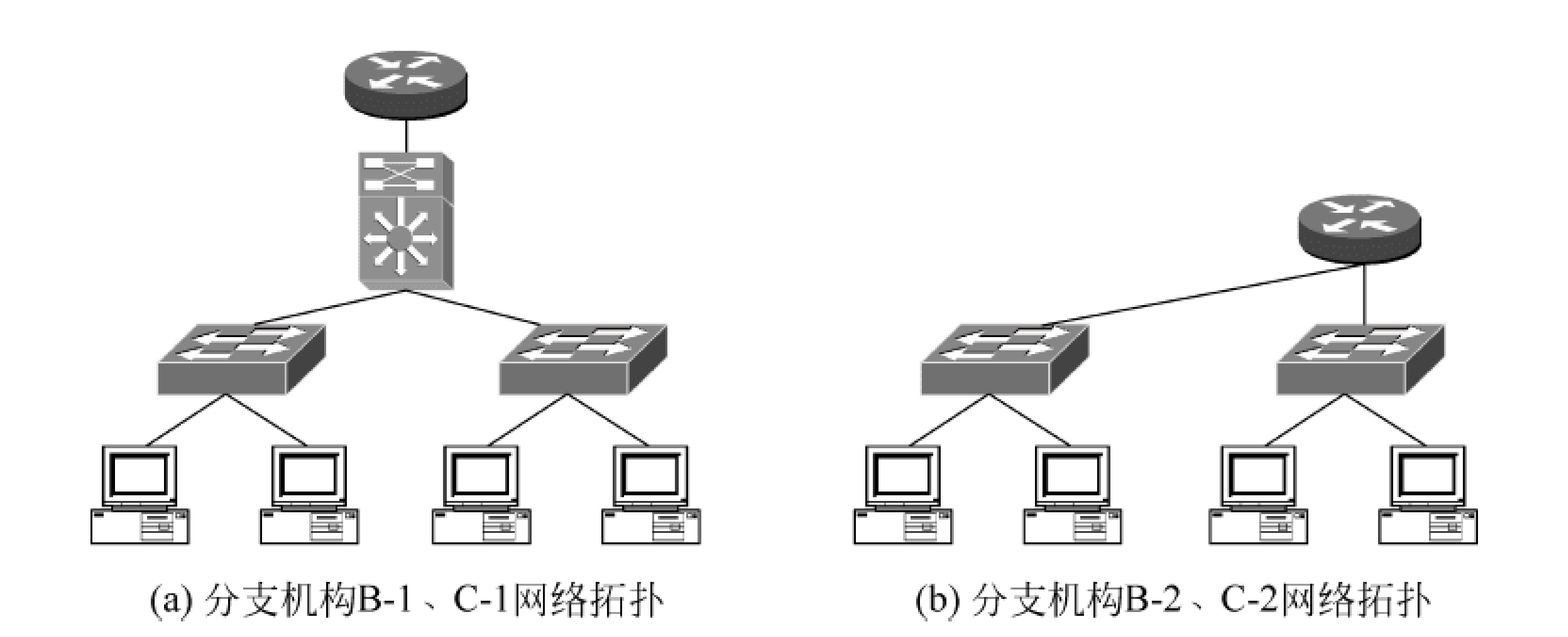


图 1-3　分支机构网络拓扑结构图

1.2　模拟公司网络安全及管理需求

1.2.1　模拟公司的网络安全管理需求

目前计算机网络面临着多方面的安全威胁，例如，物理安全威胁、网络通信威胁、网络服务威胁、网络管理威胁等，模拟公司网络也不能例外。本书将重点讨论如何解决网络通信安全威胁问题，其他方面的解决方法可参考本系列教材中的《计算机网络集成技术》和《网络操作系统》两书。

从模拟公司网络环境和业务需求分析可以发现，要保证该网络安全运行，需要解决以下网络安全问题。

(1) 由于连接到 Internet，所以必须解决来自 Internet 的网络入侵和攻击问题。

(2) 模拟公司与分支机构间使用 Internet 线路通信，必须解决通信数据安全问题。

(3) 由于公司租用的 IP 地址有限，随着企业网络规模发展，必须解决公司网络中 IP 地址资源不足的问题。

(4) 模拟公司网络不是单纯的生产网络，办公局域网的接入，使得网络管理人员必须面对局域网中各种潜在安全威胁，如病毒问题、非授权访问网络资源问题、非授权变更网络结构等。

1.2.2　模拟公司的网络管理需求

要保证模拟公司网络安全、可靠运行，必须对网络进行管理和维护。在网络管理过程中，需要解决以下问题。

(1) 根据网络需求变化，使用工具对网络进行配置、调整。

(2) 当网络发生故障时，能够发现、跟踪故障现象，记录故障状态信息，分析故障原因，解决网络故障。

(3) 监控、记录网络性能变化；根据网络需求适当调整网络，以提高网络性能。

(4) 监控、记录网络受到安全威胁的情况，检查网络可能存在的安全漏洞或隐患，并通过访问控制等手段对网络的薄弱环节进行改善。

1.3 网络安全及管理实验环境

本书将根据以上网络安全及管理方案基本设计思路，逐个解决模拟公司网络中的安全及管理方面的问题，介绍相关知识，提出解决方案，完成相应系统配置。在课程学习过程中，可在如图 1-4 所示实验环境中进行相应配置，测试网络安全及管理方案的可行性。

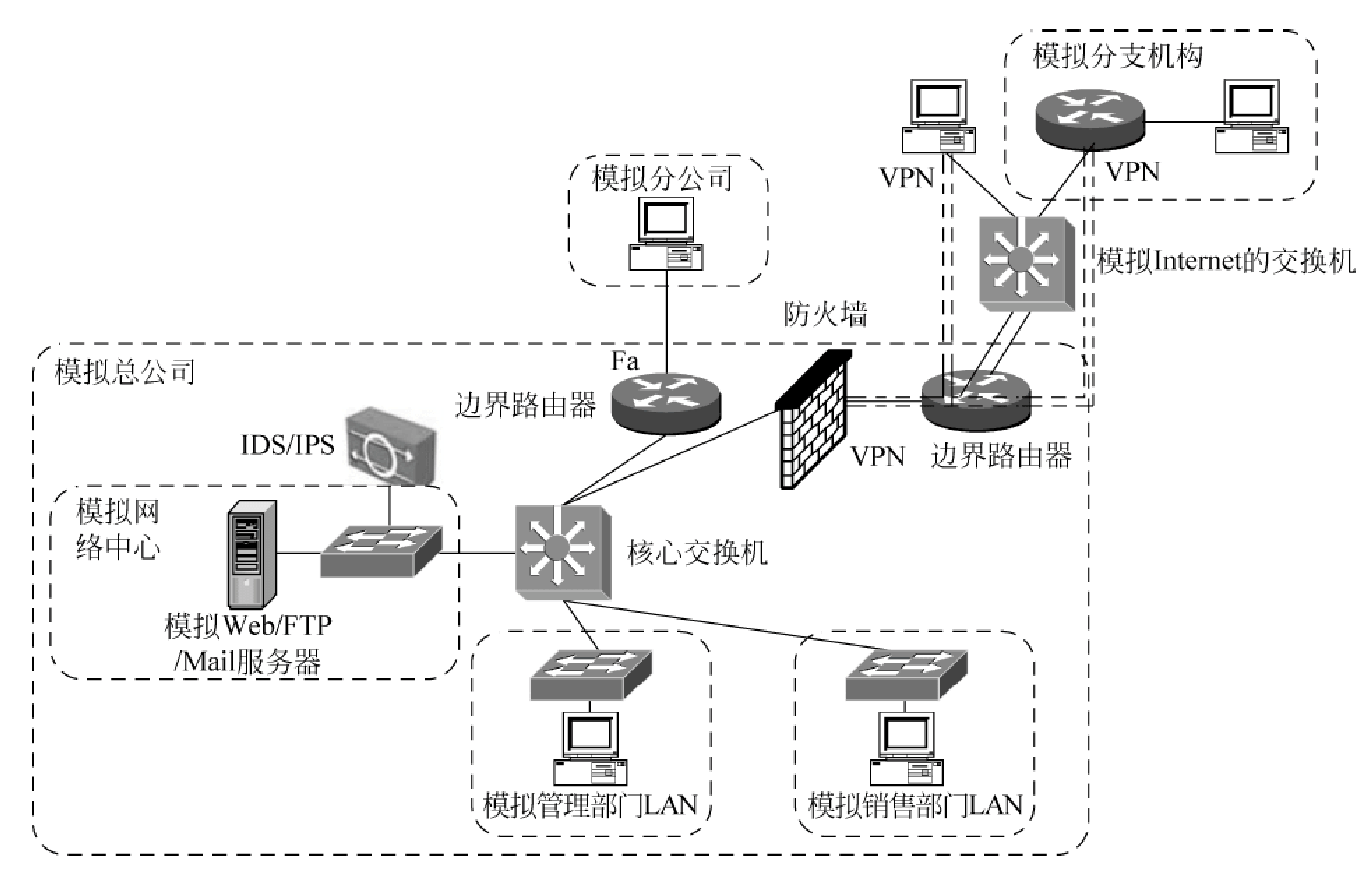


图 1-4 实验网络拓扑结构图

图 1-4 所示的实验网络拓扑可使用实际网络设备实现，也可使用模拟器软件实现。为便于实验，简化与网络安全、管理无关的内容，网络中广域网线路可使用以太网线路或串行口的背对背线路进行模拟；图中的 IDS/IPS 设备也可使用安装 IDS 软件的计算机模拟。

该模拟网络实验环境的硬件系统包括如下内容。

(1) 防火墙。

(2) IDS 设备(可选)。

(3) 路由器。

(4) 二层、三层交换机。

(5) PC。

该模拟网络实验环境的软件系统包括如下内容。

(1) Web、FTP、Mail 服务软件。

(2) IDS 软件。

(3) VPN 客户端软件。

(4) 网络管理软件，例如 PRTG 等。

(5) 网络攻击软件，例如 Smurf 等。

第 2 章

访问控制列表技术

本章任务：根据工程任务安全需求分析，解决网络边界访问控制配置问题。

必备知识：(1) 无状态访问控制列表技术。

(2) 有状态访问控制列表技术。

(3) 基于上下文的访问控制列表技术。

学习目标：利用访问控制列表技术完成模拟公司分支机构网络边界访问控制配置，防御外网攻击。

2.1 模拟公司分支机构网络边界安全任务分析

2.1.1 模拟公司分支机构网络边界安全风险分析

如图 2-1 所示，模拟公司各分支机构网络通过 Internet 与模拟公司其他网络相连，各分支机构网络内设有可 24 小时连接到 Internet 的邮件服务器，周一至周五使用端口 3000～3010 通过 Internet 连接总/分公司的应用服务器，24 小时可通过 Internet SSH 连接远程管理的网络设备。由于 Internet 的开放性，各分支机构网络面临以下安全风险。

1. 恶意用户对分支网络进行的勘测攻击

勘测攻击是一种对网络进行扫描或窃听，试图获得网络拓扑、网络中主机或网络设备运行应用软件情况的攻击方式，它往往是恶意用户对网络实施攻击的前奏。勘测攻击的两种常见类型是扫描和窃听。

常见扫描攻击包括 IP 地址扫描和端口扫描。通过 ping 网络的直接广播地址或者 ping 网络中每个 IP 地址，恶意用户就可以对网络实施 IP 地址扫描；而一些常用端口扫描工具，也可以通过测试是否可以与网络中主机建立各类服务连接来探测主机上打开的网络服务端口情况。

勘测攻击的另一种类型是窃听攻击。恶意用户可以通过各类嗅探、监听软件，从网络流量中窃取用户账户等信息。但此类攻击一般只能在本地网络中实施。恶意用户往往通过先攻陷网络内部一台主机，然后在这台主机上运行嗅探、监听软件，来进行此类攻击。

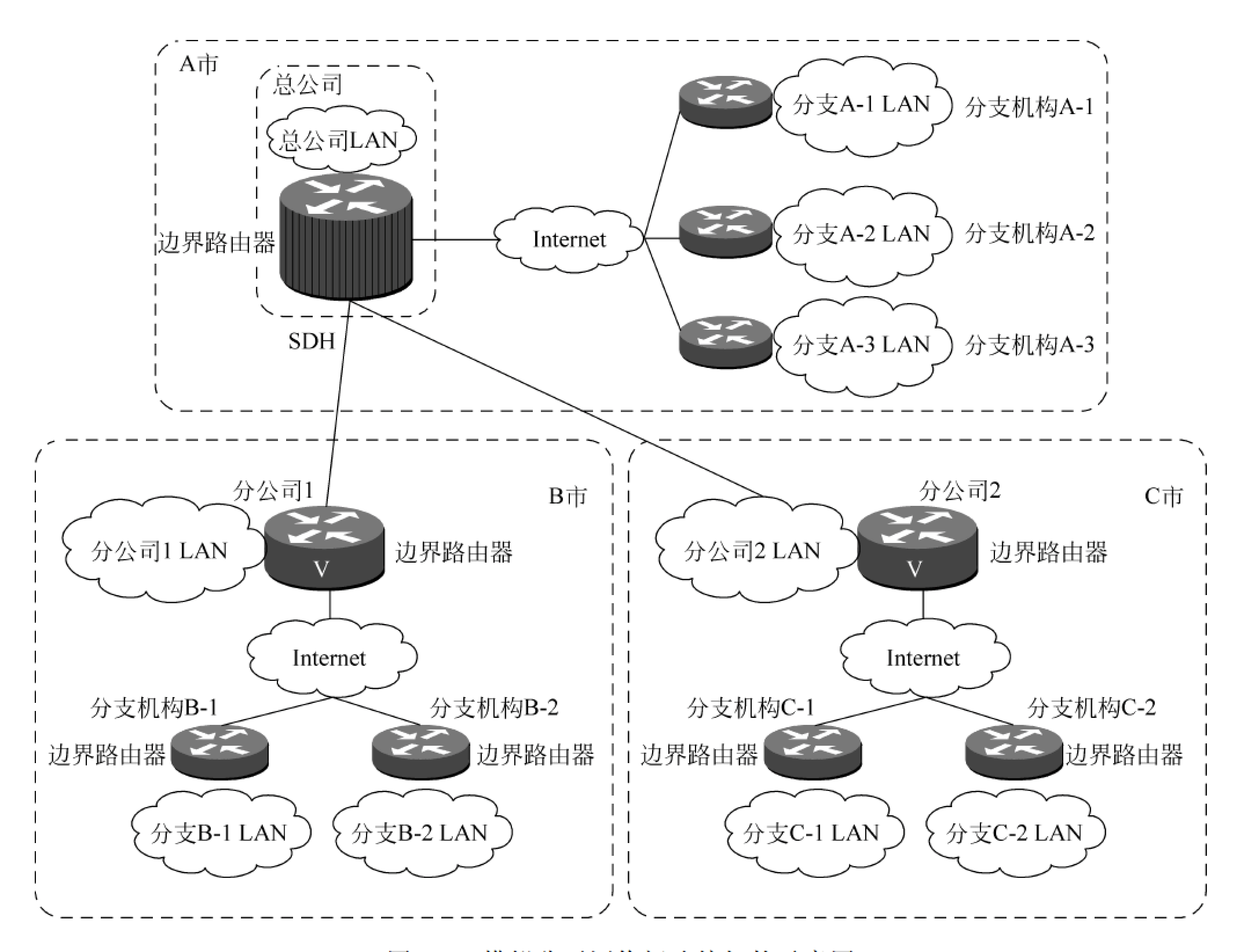


图 2-1 模拟公司网络间连接拓扑示意图

2. 恶意用户对分支网络进行的访问攻击

访问攻击常见类型包括未授权访问攻击、数据操纵攻击、会话攻击等。

(1) 未授权攻击是指通过口令暴力破解、社会工程学窃取口令等试图获得访问网络权利的攻击方式。

(2) 数据操纵攻击是指对网络服务提供的数据内容进行修改，例如改变网页内容，嵌入非法插件、Java 小程序等。

(3) 会话攻击是指在会话层实施的网络攻击，主要类型包括会话欺骗攻击、会话重放攻击、会话劫持攻击。

① 会话欺骗攻击是指通信会话中假冒其他 IP 地址的攻击行为，如图 2-2 所示。据统计，大约 65％的会话欺骗攻击使用 bogon 地址（即未被分配的地址），包括保留地址、私有 IP 地址等；另外恶意用户常假冒内网合法主机发动会话欺骗攻击。

② 会话重放攻击是指通过监听网络中某台主机的数据报文信息，然后伪造数据报文发送给该主机的攻击行为。例如，恶意用户可以监听用户在线交易信息，然后伺机发送假冒信息给用户，误导用户登录假冒在线交易、网上银行网站。会话重放攻击如图 2-3 所示。

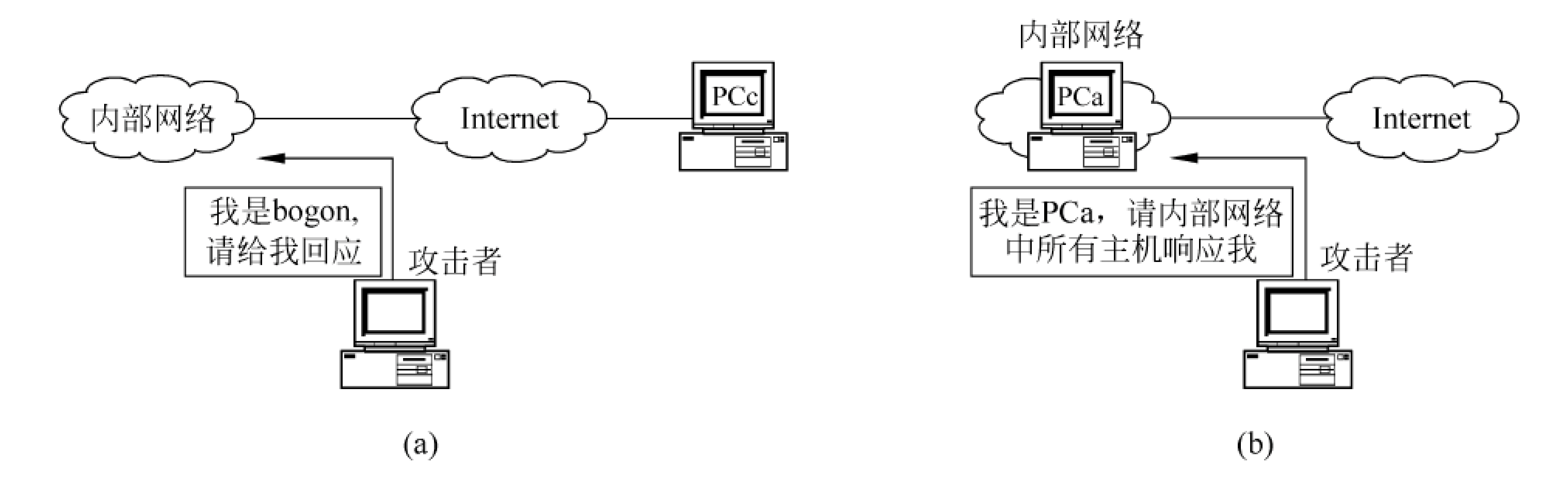


图 2-2　会话欺骗攻击示意图

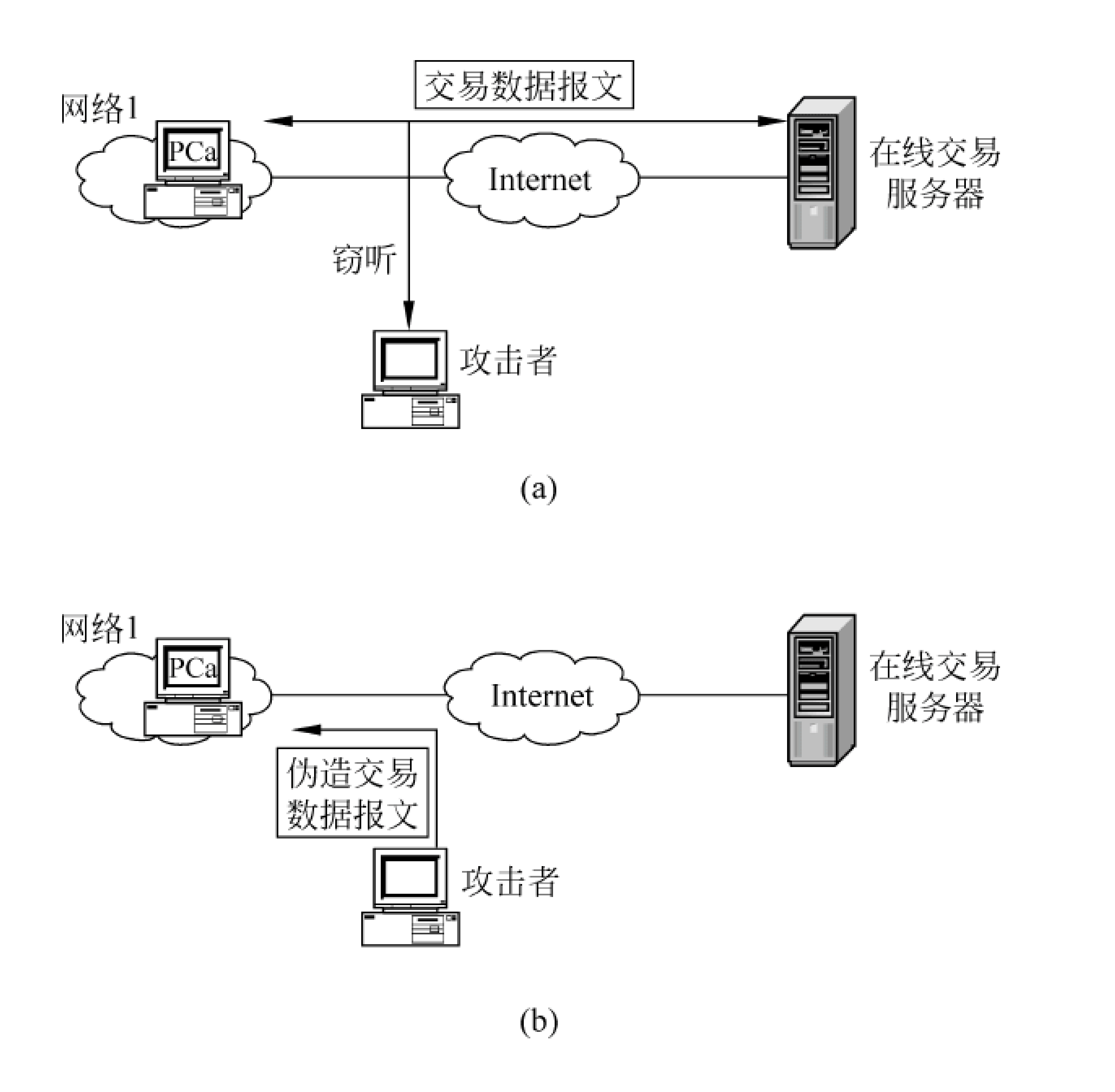


图 2-3　会话重放攻击示意图

③ 会话劫持攻击是指恶意用户拦截网络中会话信息，假扮通信双方发送虚假信息的攻击行为，如图 2-4 所示。

3. 恶意用户对分支网络进行的 DoS 攻击

恶意用户通过向网络中的网络设备、主机发送大量消耗、占用其资源的流量，使得网络、网络设备、主机无法进行正常通信的攻击行为，称为 DoS(Deny of Service)攻击。

TCP SYN 洪水攻击是一种利用 TCP 协议安全漏洞进行的 DoS 攻击，恶意用户利用 TCP 连接建立过程中“三次握手”的安全漏洞，向被攻击者发送大量连接建立请求，由于 TCP 协议需要等待接收到后续响应报文才能完成连接建立过程，大量连接建立请求会导致被攻击者大量资源被占用，无法进行正常通信。

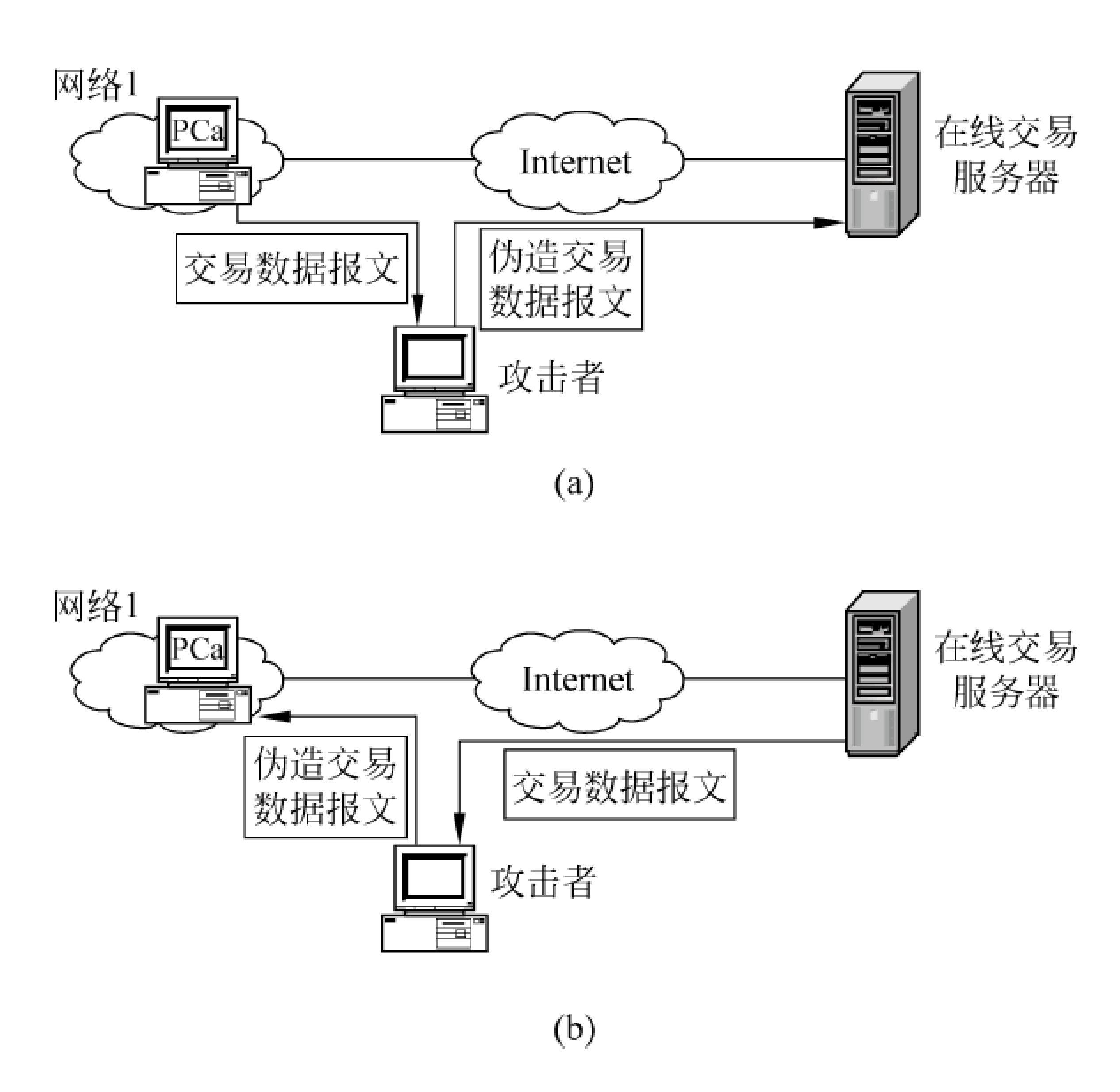


图 2-4 会话劫持攻击示意图

Smurf 攻击是一种利用 ICMP 报文洪水进行的 DoS 攻击。恶意用户可假冒被攻击主机向某网络广播地址发送 ICMP echo 报文，由于每个目的网络主机都向被攻击主机返回 ICMP reply 报文，所以会导致被攻击主机 CPU 和网络带宽被大量占用而不能再正常提供服务。

4. 恶意用户对分支网络进行的 DDoS 攻击

DDoS(Distributed Denial of Service)攻击即分布式拒绝服务攻击，是从多个源头发动 DoS 攻击的攻击方式。恶意用户往往先通过其他手段攻陷若干防御薄弱的主机，在其上安装可以远程控制的攻击程序，使其成为“肉机”，然后再控制这些“肉机”向网络上的合法服务器发动 DoS 攻击。由于发出 DoS 攻击洪水的“肉机”位置比较分散，因此极大增加了防御该类攻击的难度。例如 TFN、TFN2K、Trinoo、特洛伊木马等。

目前防范 DoS 攻击和 DDoS 攻击的手段主要有两种：控制流量大小、禁止来自 Internet 可能对内部网络造成攻击的流量。

例如，可以通过限制来自 Internet 的 ICMP 报文进入内部网络来防范 Smurf；也通过限制 Internet 对内部网络主机的主动 TCP 连接，来防范 TCP SYN 等。

虽然 DDoS 攻击比 DoS 攻击更难防御，但大部分 DDoS 程序都有各自通信特征的特点。例如，DDoS 程序 TFN 使用 ICMP echo-reply 消息来传递“攻击指令”；DDoS 程序 Trinoo 使用比较固定的端口，如 TCP 和 UDP 的 1524、27444、27665、31335 进行通信；DDoS 程序 Trinity 使用 IRC 通信来传送攻击命令；特洛伊木马使用一些特定端口通信。

因此，如果内部网络不需要提供以上端口的网络服务，就可以在网络边界上过滤以上特定端口的流量，从而减少遭遇网络攻击的风险。

2.1.2　模拟公司分支机构网络边界安全配置方案

在边界路由器上配置访问控制列表是保护内部网络防御以上安全风险的主要手段之一。但并不是所有路由器都支持高级访问控制列表技术，因此根据模拟公司各分支机构实际配置情况，对于使用中高端路由器的分支机构可以选用方案 1 来配置边界路由器，而使用低端路由器的分支机构可以选用方案 2 来配置边界路由器。

方案 1

（1）在网络边界上配置基于上下文的访问控制列表 CBAC（Context-based Access Control），过滤来自 Internet 到内网主机或服务器的所有 ICMP echo 报文，来防御利用 ping 进行的扫描攻击。

（2）在网络边界上配置标准访问控制列表，过滤所有来自 Internet 的源地址为 bogon 地址或内网地址的访问，防御 IP 欺骗攻击。

（3）在网络边界上配置基于上下文的访问控制列表，防范 DoS 攻击。

- 限制来自 Internet 的 ICMP 报文进入内部网络，以防范 Smurf。
- 限制 Internet 对分支机构网络主机的主动 TCP 连接、UDP 连接，来防范 TCP SYN 等。

（4）在网络边界上配置扩展访问控制列表，防范使用特定协议消息、特定端口的 DDoS 攻击。

- 阻塞 ICMP echo-reply 消息，以抵御 TFN 攻击。
- 禁止 TCP 和 UDP 1524、27444、27665、16660、65000、31335 端口的流量，以防御 Trinoo 等 DDoS 攻击。
- 禁止 TCP 端口 6665～6669 的 IRC 流量以防御 Trinity 攻击。
- 禁止常见特洛伊木马使用的特定端口。

方案 2

对于那些不支持 CBAC 功能的路由器，配置反射访问控制列表作为替补方案。

（1）在网络边界上配置反射访问控制列表，过滤来自 Internet 到内网主机或服务器的所有 ICMP echo 报文，来防御利用 ping 进行的扫描攻击。

（2）在网络边界上配置标准访问控制列表，过滤所有来自 Internet 的源地址为 bogon 地址或内网地址的访问，防御 IP 欺骗攻击。

（3）在网络边界上配置基于上下文的访问控制列表，防范 DoS 攻击。

- 限制来自 Internet 的 ICMP 报文进入内部网络，以防范 Smurf。
- 限制 Internet 对分支机构网络主机的主动 TCP 连接、UDP 连接，来防范 TCP SYN 等。

（4）在网络边界上配置扩展访问控制列表，防范使用特定协议消息、特定端口的 DDoS 攻击。

- 阻塞 ICMP echo-reply 消息，以抵御 TFN 攻击。
- 禁止 TCP 和 UDP 1524、27444、27665、16660、65000、31335 端口的流量，以防御 Trinoo 等 DDoS 攻击。
- 禁止 TCP 端口 6665～6669 的 IRC 流量以防御 Trinity 攻击。

- 禁止常见特洛伊木马使用的特定端口。

方案 1 和方案 2 中提及的 bogon 地址，可以检索 http://www.cymru.com/Documents/bogon-dd.html 网页获得；常见木马端口可从 http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html 获得。表 2-1 显示了截至 2009 年 8 月 Internet 上的 bogon 地址。

表 2-1 bogon 地址示例

网络地址	子网掩码	网络地址	子网掩码
0.0.0.0	254.0.0.0	100.0.0.0	252.0.0.0
2.0.0.0	255.0.0.0	104.0.0.0	252.0.0.0
5.0.0.0	255.0.0.0	127.0.0.0	255.0.0.0
10.0.0.0	255.0.0.0	169.254.0.0	255.255.0.0
14.0.0.0	255.0.0.0	172.16.0.0	255.240.0.0
23.0.0.0	255.0.0.0	176.0.0.0	254.0.0.0
27.0.0.0	255.0.0.0	179.0.0.0	255.0.0.0
31.0.0.0	255.0.0.0	181.0.0.0	255.0.0.0
36.0.0.0	254.0.0.0	185.0.0.0	255.0.0.0
39.0.0.0	255.0.0.0	192.0.2.0	255.255.255.0
42.0.0.0	255.0.0.0	192.168.0.0	255.255.0.0
46.0.0.0	255.0.0.0	198.18.0.0	255.254.0.0
49.0.0.0	255.0.0.0	223.0.0.0	255.0.0.0
50.0.0.0	255.0.0.0	224.0.0.0	224.0.0.0

2.2 访问控制列表的基础知识

2.2.1 访问控制列表的概念

访问控制列表(Access Control List，ACL)是一种过滤工具，普遍用于各种网络设备(路由器、交换机、防火墙等)中。

ACL 工作的基本原理如下。

- 定义一个访问控制列表，该访问控制列表包含一组过滤条件。
- 在网络设备接口、线路上，应用该访问控制列表对“进/出”该接口的流量进行过滤。

一个访问控制列表中包含一组命令(或称过滤条目、访问控制语句)，每条命令典型结构为：

permit | **deny** 匹配条件

即“允许”(permit)或“拒绝”(deny)符合“匹配条件”的流量通过网络设备接口。

其中“匹配条件”部分可以包含多种信息。

- 源地址或目的地址(可以是 IP、MAC 等)。
- 第 2 层协议信息，例如以太网帧类型。

- 第 3 层协议类型，例如 IP、IPX。
- 第 3 层协议信息，例如 IP、ICMP 等。
- 第 4 层协议信息，例如 TCP、UDP 端口号等。

以要隔绝图 2-5 中网络 1 和网络 2 间的 IP 流量，但不影响网络 1、网络 2 与 Internet 间访问为例，可以设计如下访问控制条目，然后应用在从路由器 Router1 接口 2 离开路由器的流量上。

- 拒绝所有来自网络 2 的流量。
- 允许所有其他流量。

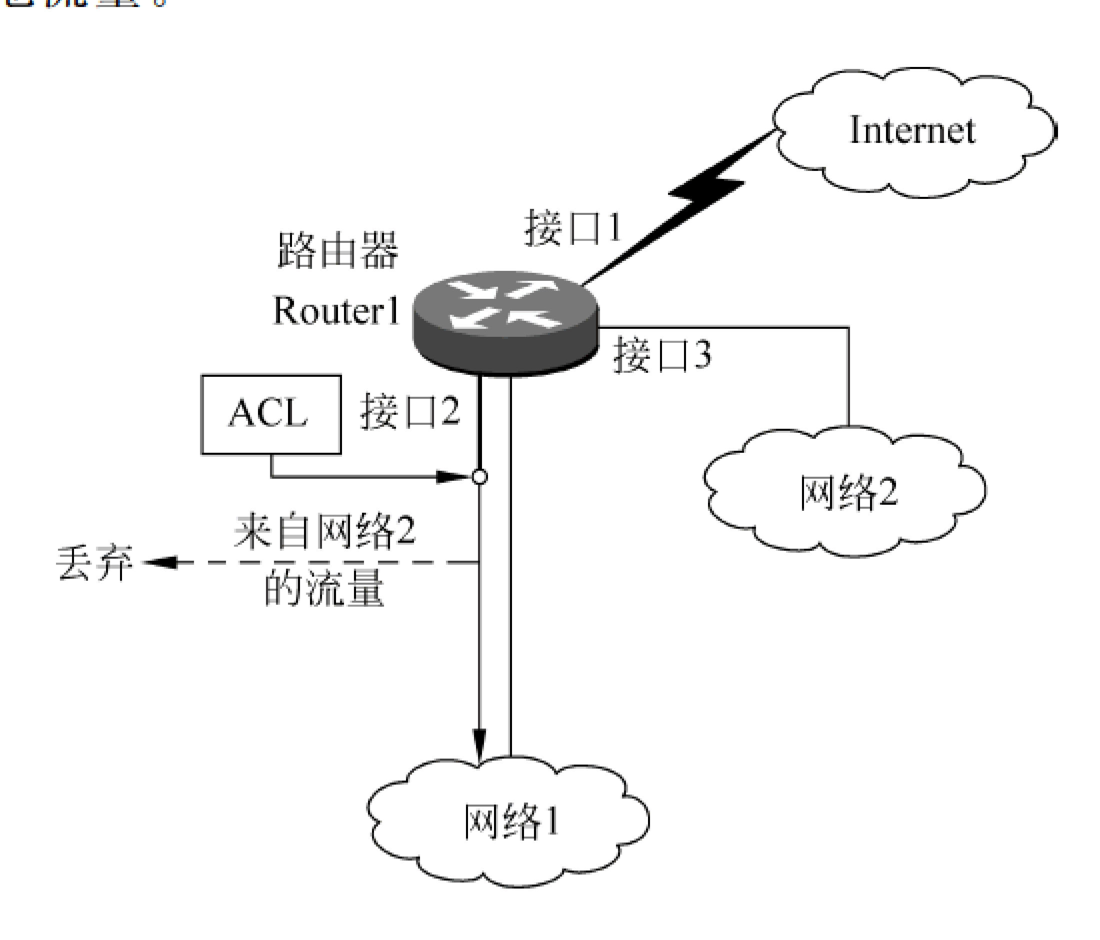


图 2-5　ACL 过滤流量示例

2.2.2　ACL 类型

ACL 有很多类型，常见的 ACL 如下。

(1) 标准 ACL(Standard ACL)：只能根据第 3 层信息来过滤流量，且只对流量来源进行过滤。通常用于限制通过 VTY 线路或者通过 HTTP、HTTPS 对网络设备的访问。

(2) 扩展 ACL(Extended ACL)：可以根据第 3 层、第 4 层信息来过滤 IP 流量，且对流量来源、目的地均可进行过滤。

(3) 定时 ACL(Time-range ACL)：是一种扩展 ACL，并且还可以定义什么时间段 ACL 被激活。

(4) 反射 IP ACL(Reflect ACL)：根据第 5 层会话信息来过滤 IP 流量。

(5) 基于上下文的 ACL(CBAC ACL)：可以根据第 3～7 层信息过滤 IP 流量。

(6) 锁和密钥 ACL(Lock-and-Key ACL)：可以根据第 3 层、第 4 层信息来过滤 IP 流量，允许用户用验证机制控制访问一个特定的源/目的地。

2.2.3　ACL 工作过程

数据报文在路由器中 ACL 和路由的处理顺序如图 2-6 所示。从接口进入路由器的数据报文，先经入站 ACL 处理，然后再做路由；而对于从接口送出路由器的数据报文，则一定已经做过路由处理，此时如果送出接口上有出站 ACL，还需要进行出站 ACL 处理。

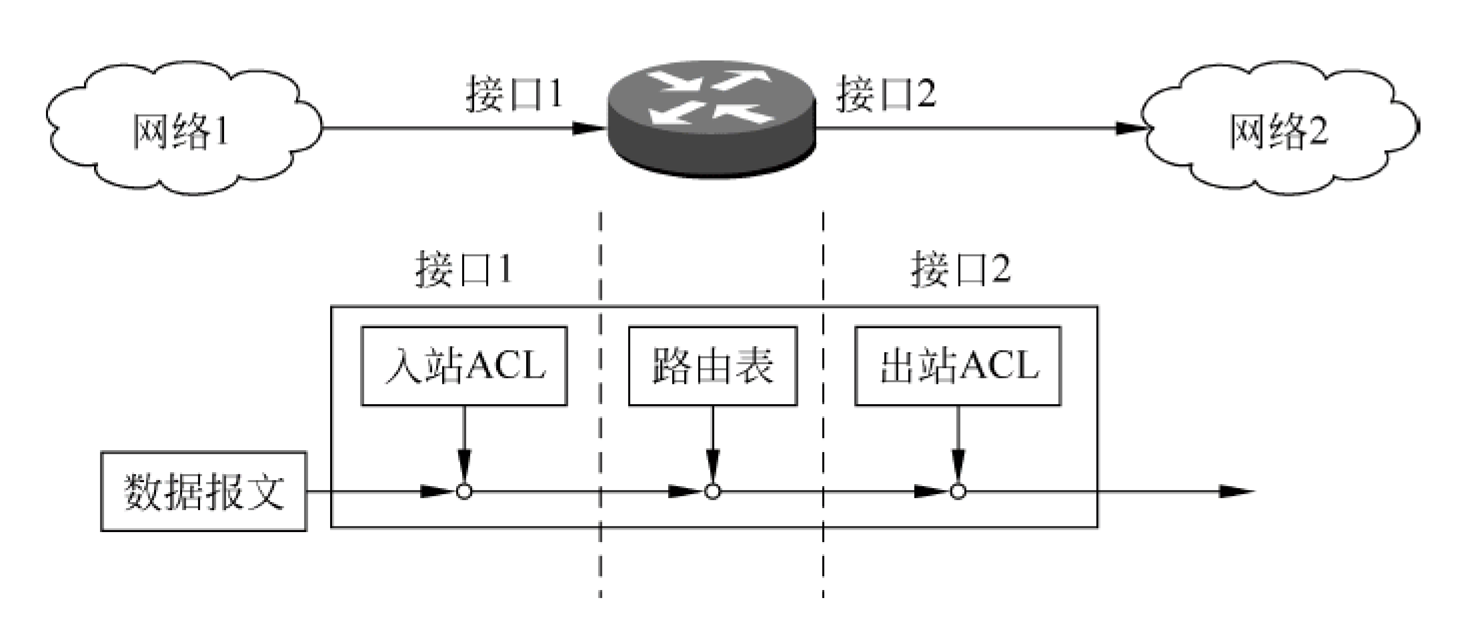


图 2-6 数据报文在路由器中的处理过程

数据报文被入站、出站 ACL 过滤的处理流程如图 2-7 所示。当数据报文在路由器接口上碰到 ACL 时，路由器会自顶向下顺序在 ACL 中检查是否有相匹配的过滤条目，如果找到一条匹配的过滤条目，就停止向下继续检查其他过滤条目，并将该数据报文按所匹配的过滤条目定义进行处理。但如果遍历整个 ACL，也未找到匹配的过滤条目，则路由器会将该数据报文丢弃。

2.2.4 ACL 配置规则和应用位置

1. ACL 的配置规则

在 Cisco 网络设备上定义 ACL 时，必须遵循以下规则。

(1) Cisco 网络设备上一组过滤条目保存在一个 ACL 中，该 ACL 在网络设备中由一个唯一的编号或名称来标识。

(2) 每条过滤条目只能配置一个匹配条件和相应处理操作(即要么允许、要么拒绝)。因此当需要控制多个匹配条件或者多个处理操作时，需配置多条过滤条目。

(3) ACL 中过滤条目的顺序非常重要。由于网络设备是从 ACL 顶部开始向下进行匹配的，一条匹配不上，就接着取其下面一条语句进行匹配，而找到一条匹配的过滤条目，就不会再继续寻找下面的过滤条目，所以每个 ACL 中的过滤条目应按照其约束性强弱，将约束性最强的放在列表的顶部，约束性最弱的语句放在列表的底部，来保证访问控制能被有效地执行。

(4) 在 Cisco 设备上，每个 ACL 最后都会自动增加一个隐式拒绝所有报文的过滤条目，所以每个 ACL 中至少有一个允许操作，否则所有数据报文都会被拒绝。

注意：并不是所有品牌的网络设备都自动增加隐式拒绝过滤条目，H3C 网络设备中的 ACL 则正好相反。

(5) 如果一个 ACL 中没有定义任何过滤条目，就被称为一个空 ACL。将一个空 ACL 应用到网络设备接口或线路上，则该空 ACL 中的隐式拒绝过滤条目不会起作用，它将允许所有数据报文通过。

(6) 将一个 ACL 应用到接口或线路上，称为激活该 ACL。每个接口的一个方向(入站或出站)上只能应用一个 ACL。

(7) 在数据包经路由器某接口进入路由器，并将被路由到其他接口之前，路由器将处理该接口上的入站 ACL。

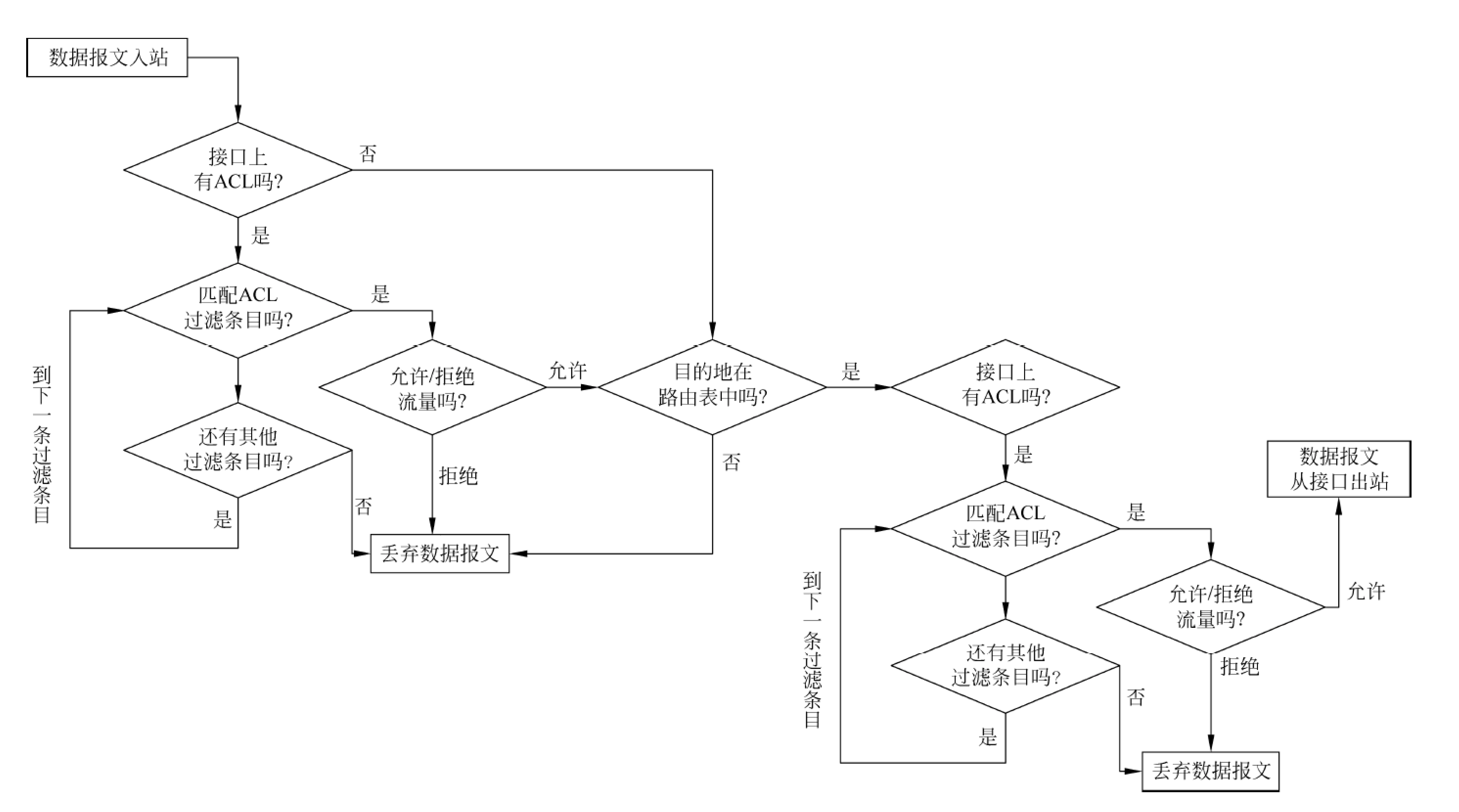


图 2-7　数据报文入站、出站 ACL 处理流程

(8) 在数据包被路由到某接口,并经该接口离开路由器之前,路由器将处理该接口上的出站 ACL。

(9) 路由器在丢弃被过滤掉的数据报文时,会生成 ICMP 管理性禁止信息。

(10) 路由器并不过滤路由器本身产生的流量。

2. ACL 的应用位置选择

在设计使用 ACL 过滤网络流量时,必须考虑 ACL 将要应用在哪个网络设备的哪个接口的哪个方向的流量上,即恰当选择 ACL 的应用位置。

虽然在实际生产中 ACL 的应用位置是根据访问控制需求确定的,但在尽可能早将无用流量丢弃以节省网络资源,同时又能保证合理流量正常通过网络设备的前提下,仍然可以遵循以下两个规则来设计 ACL 的应用位置。

规则 1:只根据数据报文源地址进行过滤的 ACL,例如标准 ACL,应放在离数据报文的目的地尽可能近的地方。

规则 2:根据数据报文中的源地址信息、目的地址信息、源端口、目的端口等多种信息进行过滤的 ACL,例如扩展 ACL,应放在离数据报文源地址尽可能近的地方。

以图 2-8 为例,如果要设计一个 ACL 以禁止除网络 1 外其他网络对 Router1 的 Telnet 访问,则可以在 Router1 的 TTY 线路上应用一个标准 ACL,只允许来自网络 1 的数据报文通过。

而如果要禁止图 2-8 中网络 2 对网络 1 的 HTTP 访问流量,则较好的解决方法是在 Router2 接口 3 的入站方向上应用一个扩展 ACL 拒绝目的地址是网络 1 的 TCP 流量。

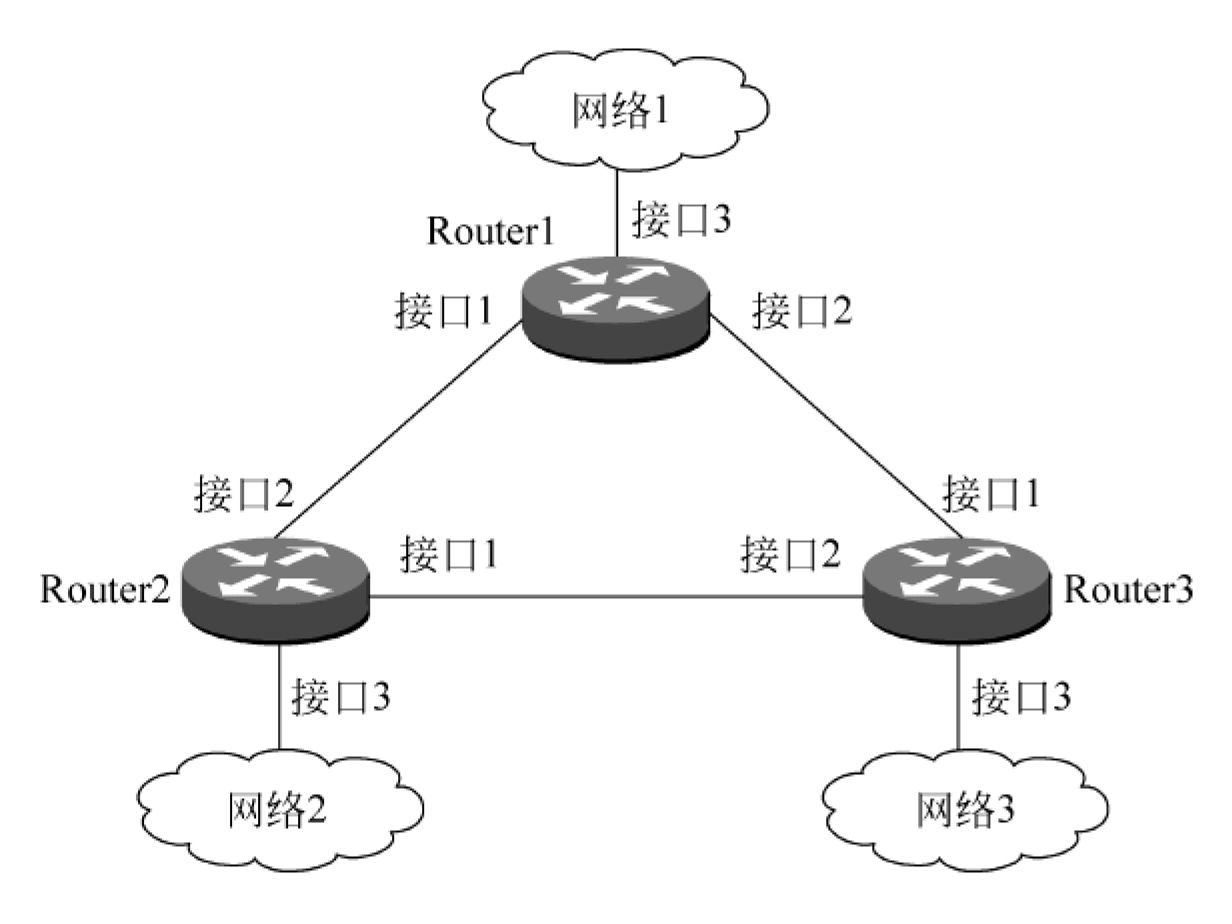


图 2-8 ACL 应用位置示例

2.3 无状态 ACL 配置方法

2.3.1 标准 ACL 配置步骤

在 Cisco 网络设备上配置标准 ACL 的基本步骤及命令如表 2-2 所示。

表 2-2　标准 ACL 配置步骤及相关命令

序　号	操　　作	相关命令	是否必要
步骤 1	定义标准 ACL	**access-list** 或 **ip access-list**	是
步骤 2	在接口或线路上应用 ACL	**ip access-group**	是
步骤 3	检查 ACL 配置和应用情况	**show access-list** **show ip interface**	可选

1. 使用 access-list 命令定义标准 ACL

Cisco 网络设备上的 access-list 命令用于定义编号标准 ACL 或编号扩展 ACL。access-list 命令在全局配置模式下使用，其语法如下。

access-list **ACL** 编号 ｛ **deny** ｜ **permit** ｝ 匹配条件

(1) ACL 编号

access-list 命令一次只能定义一个 ACL 中的一条过滤条目。当一个 ACL 中存在多条过滤条目时，可以使用多条相同“ACL 编号”的 access-list 命令来实现，并且先定义的条目位于 ACL 顶部，后定义的过滤条目自动追加到 ACL 的尾部。

access-list 命令中的“ACL 编号”是一个 ACL 在一台网络设备中的唯一标识，而且还有区分 ACL 类型的作用。不同编号范围对应的 ACL 类型如表 2-3 所示。要定义标准 ACL，编号可以从 1～99 或 1300～1999 的范围中选取。

表 2-3　各类访问控制列表编号范围

编号范围	ACL 类型	编号范围	ACL 类型
1～99	IP 标准访问控制列表	200～299	协议类型码访问控制列表
100～199	IP 扩展访问控制列表	2000～2699	IP 扩展访问控制列表
1100～1199	MAC 地址扩展访问控制列表	700～799	MAC 地址访问控制列表
1300～1999	IP 标准访问控制列表		

(2) ACL 操作关键字

access-list 命令中的 deny 关键字表示会拒绝匹配条件的流量；permit 关键字表示会允许匹配条件的流量。

(3) 标准 ACL 的匹配条件定义

标准 ACL 的匹配条件只需定义流量来源，其语法如下所示。

｛ **源主机地址　通配符** ｜ **any** ｜ **host　源主机地址** ｝

标准 ACL 的匹配条件定义中支持 3 种流量来源的表示方式。

- “源主机地址”参数与“通配符”参数一起使用，用于定义一定范围的源主机。源主机地址可以是源主机名或源主机 IP 地址。
- 关键字 any 指任何名字或 IP 地址的源主机。
- 关键字 host 后跟参数“源主机地址”用于指定一台源主机。

(4) 通配符

“通配符”与子网掩码类似，是一种长 32 位的二进制掩码。但与子网掩码不同的是，

通配符某位值为1,表示匹配条件中源地址对应位的值可被忽略;而某位值为0,则表示匹配条件中源地址对应位的值必须匹配。所以在某些地方,通配符也被称为“反掩码”。

例如,“所有网络200.100.10.0/24中的主机”的匹配条件可以如下定义。

```
200.100.10.0    0.0.0.255
```

通配符0.0.0.255,前24位二进制0对应匹配条件中IP地址的网络前缀部分200.100.10,表示这部分一定要匹配;最后8位为二进制1,说明最后8位可为任意值。即所有网络前缀为200.100.10的IP地址均能匹配,如图2-9所示。

主机IP地址	:	1100 1000. 0110 1000. 0000 1100. 0000 0000
通配符	:	0000 0000. 0000 0000. 0000 0000. 1111 1111
匹配的IP地址	:	1100 1000. 0110 1000. 0000 1100. xxxx xxxx

图2-9 通配符计算示例1

使用通配符时,没有像子网掩码那样0、1必须连续的限制,因此使用起来更加灵活。例如,“所有网络200.100.10.0/24中主机号为偶数的主机”可以如下定义。

```
200.100.10.0    0.0.0.254
```

即网络前缀为200.100.10.0,主机号最末位为0的主机。计算过程如图2-10所示。

主机IP地址	:	1100 1000. 0110 1000. 0000 1100. 0000 0000
通配符	:	0000 0000. 0000 0000. 0000 0000. 1111 1110
匹配的IP地址	:	1100 1000. 0110 1000. 0000 1100. xxxx xxx0

图2-10 通配符计算示例2

(5)标准编号ACL举例

例如,实现“禁止除网络200.100.8.0/128外来自其他网络IP流量”功能的标准ACL定义命令如下。

```
access-list  10  permit  200.100.8.0  0.0.0.127
```

2. 使用命令ip access-list定义标准ACL

Cisco网络设备上的ip access-list相对access-list命令,功能更强。使用ip access-list可以为ACL指定一个描述性的名称“ACL名”;还可以删除ACL中的特定条目。

ip access-list命令配置标准ACL的语法如下。

ip access-list standard {ACL名 | ACL编号}
[条目编号] {**permit** | **deny**} 匹配条件

ip access-list命令在全局模式下使用,而permit和deny为ip access-list命令的子句,需在ip access-list命令模式下才能够输入。

ip access-list命令中“条目编号”参数,用于指定当前配置条目在该标准ACL中的序号。

ip access-list命令中的“ACL名”参数,用于在网络设备上唯一标识该ACL,注意

ACL 名可以包含数字,但必须以字符开头。

ip　access-list 命令中"匹配条件"参数的用法与前述标准 ACL 匹配条件相同。

3. 在接口或线路上应用定义的 ACL

在 Cisco 网络设备接口上,应用标准或扩展 ACL 的操作相同,均为在接口配置模式下输入:

ip　access-group　ACL 编号或 ACL 名　{ **in** | **out**}

例如,如果要在路由器接口 Fa0/1 的入站流量上应用编号为 10 的标准 ACL,则可以如下配置。

```
Router1(config)# interface  fa0/1
Router1(config-if)# ip  access-group  10  in
```

在 Cisco 网络设备 VTY 线路上,应用标准 ACL 的操作为在 VTY 线路配置模式下输入:

access-class　{　ACL 编号 |　ACL 名 }　{ **in** | **out** }

例如,在 Router1 VTY 线路入站流量上,应用编号为 10 的标准 ACL 配置如下。

```
Route1r(config)# line  vty  0  4
Router1(config-line)# access-class  10  in
```

4. 检查 ACL 配置和应用情况

(1) 检查已定义的 ACL 信息

在 Cisco 上可以用 show　access-list 命令检查网络设备上所有已定义的 ACL 信息。该命令语法如下。

show　[协议]　**access-list**　[　ACL 名 |　ACL 编号]

"协议"参数可以使用 ip、ipx 等来显示特定协议的 ACL。

"ACL 名"、"ACL 编号"参数用于显示指定 ACL 的内容。

该命令及输出结果如下。

```
Router1# show  access-list
Standard IP access list 10
10 permit 200.100.10.0, wildcard bits 0.0.0.255 (4 matches)
```

结果显示了 Router1 上现在配置有 1 个标准 ACL,编号为 10,到该命令执行前,已经有 4 个数据报文匹配了该标准 ACL。

(2) 检查接口应用 ACL 情况

在 Cisco 上可以用 show ip interface 命令检查网络设备接口上应用 ACL 的情况。该命令语法如下。

show　ip　interface　接口号

参数“接口号”为应用 ACL 的接口号。

该命令使用及输出结果如下。

```
Router1# show  ip  interface  fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.10.10.1/24
  Broadcast address is 255.255.255.255
此处省略部分显示...
  Outgoing access list is not set                         ①
  Inbound  access list is eacl-out2in                     ②
此处省略部分显示...
```

从该命令输出结果中可以显示接口 Fa0/0 上应用 ACL 的情况。①显示说明在出站方向上没有应用 ACL。②显示说明在入站方向上应用了一个名为 eacl-out2in 的 ACL。

2.3.2 扩展 ACL 配置步骤

在 Cisco 网络设备上配置扩展 ACL 的基本步骤及命令与标准 ACL 相同，仅命令参数和匹配条件定义上有区别。

使用 access-list 命令定义扩展 ACL 时，要注意 ACL 编号的范围为 100～199、2000～2699。

使用 ip access-list 命令定义扩展 ACL 时，要使用 ip access-list extended ACL 名的形式，即使用 extended 关键字定义该 ACL 为扩展 ACL。

定义扩展 ACL 时，针对不同协议报文的匹配条件语法各不相同。下面为常用 IP、TCP、UDP、ICMP 流量匹配条件的语法。

1. IP 流量匹配条件

禁止或允许所有指定源地址到达指定目的地址 IP 流量的匹配条件应按如下语法定义。

ip {源地址 源地址通配符 | **any** | **host** 源地址} {目的地址 目的地址通配符 | **any** | **host** 目的地址} [**precedence** 优先级] [**tos** 服务类型域或服务名] [**log** | **log-input**] [**time-range** 时间范围名] [**fragments**]

关键字 ip 用于指定过滤 IP 流量。ip 关键字后面参数的用法与标准 ACL 定义部分相同。

“优先级”参数用于过滤特定优先级的 IP 流量，优先级范围为 0～7，对应于 IP 报头中优先级字段。

“服务类型域或服务名”参数用于过滤指定服务类型的 IP 流量。

“优先级”、“服务类型域或服务名”参数对应的 IP 报头字段都与 QoS 实施有关。

使用关键字 log 会生成有关匹配该条件的记录日志。被记录的日志信息包括允许或拒绝操作、匹配的协议、源地址和目的地址、TCP/UDP 协议的源端口号和目的端口号、ICMP 消息类型等。

注意： 使用关键字 log 会严重影响网络设备的性能，因此一般只在发现遭受网络攻击时，才会打开该功能用以确定攻击者位置。

关键字 log-input 与 log 类似,但还会记录匹配流量的输入接口和流量中第 2 层源地址,更易于定位攻击者位置。

“时间范围名”参数用于为 ACL 指定一个已经定义的时间范围。该参数用于定时 ACL 的配置。

可选参数 fragments 关键字用于分片的过滤。

2. ICMP 流量匹配条件

ICMP 流量匹配条件可以用在希望限制或允许 ICMP 流量的情况,可以使用该匹配条件定义限制从指定源地址到指定目的地址间的所有各类 ICMP 协议报文流量,也可以仅限制部分 ICMP 流量。

icmp {源地址 源地址通配符 | **any** | **host** 源地址 } {目的地址 目的地址通配符 | **any** | **host** 目的地址 } [**ICMP** 报文类型 | [**ICMP** 报文类型 **ICMP** 代码 | **ICMP** 消息] [**precedence** 优先级] [**tos** 服务类型域或服务名] [**log** | **log-input**] [**time-range** 时间范围名] [**fragments**]

例如,如果希望允许图 2-8 所示网络 1、网络 2 中主机可以使用 ping 测试到达 Internet 的连通性,但却不希望 Internet 能 ping 通网络 1、网络 2 中主机,则可以利用 ICMP 协议工作特点,在路由器接口 1 Fa0/1 入站方向上如下配置 ACL,禁止所有 Internet 对网络 1、网络 2 中主机的 ICMP echo 报文,但允许其他 IP 报文通过,该扩展 ACL 配置如下。

```
Router1(config)#ip access-list extended eacl-noicmp
Router1(config-ext-nacl)#deny icmp any any echo
Router1(config-ext-nacl)#permit ip any any
Router1(config-ext-nacl)#exit
Router1(config)#interface fa0/1
Router1(config-if)#ip access-group eacl-noicmp in
Router1(config-if)#end
```

配置完成后显示存取控制列表结果如下。

```
Router1#show access-lists

Extended IP access list eacl-noicmp
10 deny icmp any 200.100.10.0 0.0.0.255 echo
20 permit ip any any
```

3. TCP 流量匹配条件

TCP 流量匹配条件可以用于允许或禁止所有或部分指定类型的 TCP 流量通过网络设备。

tcp {源地址 源地址通配符 | **any** | **host** 源地址 } [运算符 [源端口号]] {目的地址 目的地址通配符 | **any** | **host** 目的地址 } [运算符 [目的端口号]] [**established**][**precedence** 优先级] [**tos** 服务类型域或服务名] [**log** | **log-input**] [**time-range** 时间范围名] [**ack**] [**fin**] [**psh**] [**rst**] [**syn**] [**urg**] [**fragments**]

关键字 tcp 指定只有 TCP 流量会匹配该条件定义。

“运算符”参数与“源端口号”、“目的端口号”配合用于指定 TCP 流量的“源端口号”、“目的端口号”范围。各种运算符的含义及用法举例如表 2-4 所示。

表 2-4 运算符含义及使用举例

运算符	含 义	举 例
eq	等于(equal)	**eq www** ＃所有端口号为 www 服务器端口，即 80 端口的流量
gt	大于(greater)	**gt 1023** ＃所有端口号大于 1023 的流量
lt	小于(lower)	**lt 1023** ＃所有端口号小于 1023 的流量
neq	不等于(not equal)	**neq 3389** ＃所有端口号不等于 3389 的流量
range	端口号范围	**range 0 1023** ＃所有端口号在 0～1023 之间的流量

established 关键字指定如果流量中设置了 ACK、FIN、PSH、RST、SYN、URG 标志，则匹配该条件定义。

可选参数 ack、fin、psh、rst、syn、urg 用于过滤带有相应标志位的 TCP 流量。

例如，如果希望图 2-11 中网络 1 内主机可以向 Internet 和网络 2 主动发起 TCP 连接，但却不允许 Internet 上的主机向网络 1 内主机主动发起 TCP 连接，访问网络 1 内基于 TCP 协议的网络服务，则可以在 Router1 上如下配置。

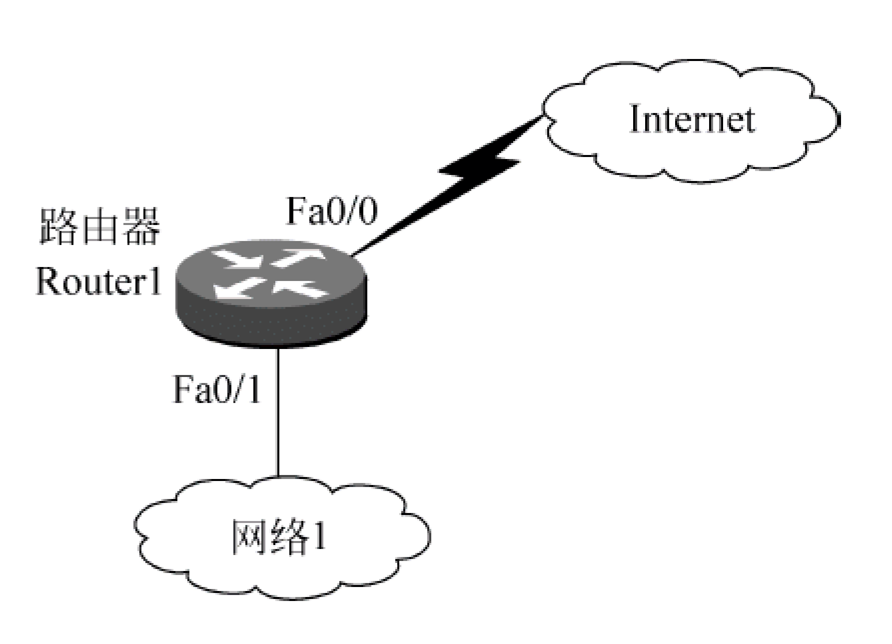


图 2-11 扩展 ACL 配置示例拓扑-TCP

```
Router1(config)＃ip access-list extended eacl-out2in                ①
Router 1(config-ext-nacl)＃permit tcp any any established           ②
Router 1(config-ext-nacl)＃deny tcp any any                         ③
Router 1(config-ext-nacl)＃permit ip any any                        ④
Router 1(config-ext-nacl)＃exit
Router 1(config)＃interface fa0/0
Router 1(config-if)＃ip access-group eacl-out2in in                  ⑤
```

以上配置说明如下。

① 创建一个名为 eacl-out2in 的扩展 ACL。

② 禁止 Internet 上的主机向网络 1 内主机主动发起 TCP 连接，可以分解为不允许建立 TCP 连接的 TCP 流量访问网络 1 内主机，但是允许响应连接建立、服务响应等 TCP 流量送达网络 1 内主机。所以对于该要求可以分解为允许已建立连接的 TCP 流量访问网络从路由器接口 Fa0/0 进入，但禁止其他的 TCP 流量，即禁止 TCP 建立连接请求流量进入。

③ 与上一条一起实现只允许已建立连接的 TCP 流量送达网络 1 内主机。

④ 由于 ACL 最后有一条隐式拒绝语句，所以为保证网络 1 与其他网络的合理通信，需要允许所有从 Internet 进入路由器接口 Fa0/0 的 IP 流量，即允许所有 IP 流量。

⑤ 作为扩展 ACL，应放在尽可能靠近流量源的地方，对于该例，最近的地方就是路

由器 Router1 的接口 Fa0/0，另外由于主要是限制 Internet 对网络 1 的访问，所以在入站方向上配置。

4. UDP 流量匹配条件

UDP 流量匹配条件用于过滤 UDP 流量。其语法如下。

udp 源地址 源地址通配符 [运算符 [端口号]] 目的地址 目的地址通配符 [运算符 [端口号]] [**precedence** 优先级] [**tos** 服务类型域或服务名] [**log** | **log-input**] [**time-range** 时间范围名] [**fragments**]

2.3.3 定时 ACL 配置步骤

在 Cisco 网络设备上，配置定时 ACL 的基本步骤及命令如表 2-5 所示。

表 2-5 定时 ACL 配置步骤及相关命令

序 号	操 作	相 关 命 令	是否必要
步骤 1	定义时间范围	**time-range**	是
步骤 2	定义 ACL	**access-list** 或 **ip access-list**	是
步骤 3	在接口或线路上应用 ACL	**ip access-group** 或 **access-class**	是
步骤 4	检查 ACL 配置和应用情况	**show access-list** **show ip interface**	可选

其中，定义时间范围的操作是在全局配置模式下输入：

time-range 时间范围名
  [**absolute** [**start** 开始时间 开始日期] [**end** 开始时间 开始日期]]
  [**periodic** 星期几 开始时间 **to** 结束时间]

absolute 和 periodic 是 time-range 命令的子命令。

absolute 用于定义单个时间范围。可以是一个起始时间或一个结束时间，或两者都有。

periodic 用于定义重复性的时间范围，即“每周什么时间到什么时间”。参数“星期几”可以使用 Monday、Tuesday、Wednesday、Thursday、Friday、daily（每天）、weekdays（周一至周五）、weekend（周六和周日）。

例如，每周一到周五早 9：00 到下午 5：00 为公司工作时间，只在该时间段允许来自 Internet 的主机访问内网一台服务器 200.100.10.10，但不允许访问其他主机。

相应的定时 ACL 和 time-range 配置如下。

```
Router1(config)# time-range tr-test
Router1(config-time-range)# periodic weekdays 9:00 to 17:00
Router1(config-time-range)# exit
Router1(config)# ip access-list extended eacl-test
Router1(config-ext-nacl)# permit tcp any host 200.100.10.10 time-range tr-test
Router1(config-ext-nacl)# permit tcp any any established
Router1(config-ext-nacl)# deny tcp any any
Router1(config-ext-nacl)# permit ip any any
```

2.3.4 分片 ACL 配置

1. 分片攻击与分片 ACL

IP 协议通过使用分片技术，解决在 MTU 最大值不同的物理网络进行数据传输的问题。当路由器要把接收到的数据包转发到使用更小 MTU 最大值的网络中时，路由器会将数据包分成符合 MTU 最大值要求的多个数据包，即分片。

但分片技术也会为网络带来安全隐患。因为网络层对传输层的数据包进行分片时，TCP 报头信息会被分到第 1 个分片中，后续的分片中却只有 TCP 数据。此时在接收设备或主机需要处理 TCP 流量而后续分片先于第 1 个分片到达的情况下，接收设备或主机会将先到的后续分片存入缓存，等待第 1 个分片到来后进行重组处理，这需要占用接收设备或主机的资源。恶意用户正是利用这种网络通信工作方式，发送大量无法重组的分片或者可以重组的无意义分片，占用接收设备或主机的资源，建立一个 DoS 攻击。

防御分片攻击有多种方案，其中一种就是使用分片 ACL 过滤掉不是数据包第 1 个分片的后续分片。

2. 分片 ACL 配置方法

在 Cisco 网络设备上使用扩展 ACL 命令中的 fragments 关键字，可以过滤分片流量。可以使用带有 fragments 关键字的 IP 流量匹配条件定义，禁止所有 IP 分片流量，可以如下配置。

```
Router1(config)# ip access-list extended eacl-test
Router1(config-ext-nacl)# deny ip any any fragments
Router1(config-ext-nacl)# permit tcp any host 200.100.10.10 time-range tr-test
Router1(config-ext-nacl)# permit tcp any any established
Router1(config-ext-nacl)# deny tcp any any
Router1(config-ext-nacl)# permit ip any any
```

也可以分别定义禁止分片的 TCP 流量、UDP 流量、ICMP、IGMP 流量等，配置如下。

```
Router1(config)# ip access-list extended eacl-test
Router1(config-ext-nacl)# deny tcp any any fragments
Router1(config-ext-nacl)# deny udp any any fragments
Router1(config-ext-nacl)# deny icmp any any fragments
Router1(config-ext-nacl)# deny igmp any any fragments
Router1(config-ext-nacl)# permit tcp any host 200.100.10.10 time-range tr-test
Router1(config-ext-nacl)# permit tcp any any established
Router1(config-ext-nacl)# deny tcp any any
Router1(config-ext-nacl)# permit ip any any
```

但需要注意的是，对于包含第 4 层信息的 ACL，Cisco 12.0(11)和 12.2(2)以前版本的 IOS 在过滤分片时遵循的规则是：如果进行了分片，且不是第 1 个分片的流量匹配了带有 fragments 参数的 ACL，但 ACL 定义的操作是 deny，则网络设备不会丢弃该流量，而是继续检查 ACL 中的下一条过滤条目。因此如果下面的过滤条目不能将该分片过滤掉，则该分片将被允许通过。Cisco 12.0(11)和 12.2(2)以后版本的 IOS 修复了该漏洞，允许由 ACL 末尾隐含的拒绝语句禁止所有流量，包括分片流量。

2.4　有状态 ACL 配置

2.4.1　反射 ACL 简介

扩展 ACL 是无状态的 ACL，配置了扩展 ACL 的网络设备只是根据数据报文中的标志、类型等过滤流量，并不记录通信过程，因此不能用于防范恶意用户利用各类响应报文或无状态报文发动的攻击。

(1) 使用扩展 ACL 可以拒绝外网对内网的 ICMP echo 报文，但考虑到要允许内网对外网的 ping 能够成功，所以需要允许外网送到内网的 ICMP echo-reply 流量。由于扩展 ACL 只是检查 ICMP 报文类型，所以不能用于防范恶意用户使用 smurf 发送大量 ICMP echo-reply 到内网的攻击。

(2) 扩展 ACL 可以通过 established 关键字，只允许外网的响应报文进入内网，但是不能用于防范恶意用户发送大量 TCP 响应报文攻击内网。

(3) UDP 协议通信时没有建立连接的过程，不能使用类似 established 关键字的扩展 ACL 来限制外网送到内网的 UDP 流量。恶意用户可以利用这一安全漏洞，使用像 Fraggle 这样的工具，向内网发送大量 UDP 报文进行 DoS 攻击。

反射 ACL 技术是一种解决以上安全问题的简易手段。

反射 ACL 技术的基本原理是：来自有效源主机的流量会触发(反射)一个允许该连接返回流量的临时 ACL，允许该连接的返回流量进入网络。

一旦反射 ACL 被产生，则会自动启动一个定时器，超时后反射 ACL 失效。

2.4.2　反射 ACL 配置方法

配置反射 ACL 的步骤如表 2-6 所示，主要配置工作包括：在路由器到外网方向上定义带有 reflect 关键字的 ACL 过滤条目，使之能产生允许返回流量的 ACL，然后在路由器到内网方向上定义带有 evaluate 命令的 ACL 过滤条目，在入站方向上指定反射 ACL 过滤条目的正确位置。

表 2-6　反射 ACL 配置步骤

序　号	操　　作	相关命令	必要性
步骤 1	定义从内网到外网的 ACL，并在需要允许返回流量的命令后增加 reflect	**ip access-list permit...reflect**	是
步骤 2	定义从外网到内网的 ACL，引用反射 ACL	**ip access-list evaluate...**	是
步骤 3	在网络设备接口上应用各方向上定义的 ACL	**ip access-group**	是
步骤 4	检查反射 ACL 配置	**show access-list** **show ip interface**	可选

如果要允许某个 permit 命令定义的流量能够产生反射 ACL，则可以输入：

permit {**tcp** ... | **udp** ...} **reflect** 反射 ACL 过滤条目名 **timeout** 超时时间

该命令将为匹配的流量创建一个指定名字的反射 ACL 过滤条目，以允许相应返回的流量。

参数“超时间隔”用于指定多长时间后该反射 ACL 失效。单位为秒，范围为 1～2147483，默认值为 300。

在配置外网到内网方向上的 ACL 中，引用所定义反射 ACL 条目的操作为在该 ACL 配置模式下输入：

```
evaluate  反射 ACL 过滤条目名
```

需要注意的是，Cisco 网络设备不会在反射 ACL 过滤条目末尾隐含增加拒绝所有流量的语句。

为限制外网主动发起向内网 TCP 连接以及向内网主动发送 UDP 报文，配置如下。

```
Router1(config)# ip access-list extended in2out                                      ①
Router1(config-ext-nacl)# permit tcp any any reflect racl-tcp                        ②
Router1(config-ext-nacl)# permit udp any any reflect racl-udp timeout 30             ③
Router1(config-ext-nacl)# permit ip any any                                          ④
Router1(config-if)# exit
Router1(config)# ip access-list extended out2in                                      ⑤
Router1(config-ext-nacl)# evaluate racl-tcp                                          ⑥
Router1(config-ext-nacl)# evaluate racl-udp                                          ⑦
Router1(config-ext-nacl)# deny tcp any any                                           ⑧
Router1(config-ext-nacl)# deny udp any any                                           ⑨
Router1(config-ext-nacl)# permit ip any any                                          ⑩
Router1(config-if)# exit
Router1(config)# interface fa0/1
Router1(config-if)# ip access-group out2in in                                        ⑪
Router1(config-if)# ip access-group in2out out                                       ⑫
Router1(config-if)# end
Router1# show ip access-lists
Extended IP access list in2out
    10 permit tcp any any reflect racl-tcp (123 matches)
    20 permit ip any any (19 matches)
Extended IP access list out2in
    20 evaluate racl-tcp
    30 deny tcp any any (39 matches)
    40 permit ip any any (62 matches)
Reflexive IP access list racl-tcp
     permit tcp host 200.100.10.2 eq telnet host 10.10.10.2 eq 11002 (45 matches)    ⑬
(time left 296)
```

以上配置说明如下。

① 定义一个名为 in2out 的扩展 ACL，该 ACL 将用于从内网到外网的流量过滤。根据安全需求，不禁止任何从内网到外网的 IP 流量，但需要检查内网到外网的 TCP、UDP 流量，以触发生成反射 ACL。

② 该过滤条目用于产生反射 ACL 以允许从外网到内网的 TCP 响应流量。

③ 该过滤条目用于产生反射 ACL 以允许从外网到内网的 UDP 响应流量，为防范恶

意用户利用定时器默认 300 秒的间隔发动 UDP 攻击，因此将定时器设置为 30 秒。

④ 该过滤条目用于允许除 TCP 流量外其他从内网到外网的 IP 流量。

⑤ 定义一个名为 out2in 的扩展 ACL，该 ACL 将用于从外网到内网的流量过滤。

⑥ 在扩展 ACL out2in 中引用允许 TCP 响应流量的反射 ACL 条目。

⑦ 在扩展 ACL out2in 中引用允许 UDP 返回流量的反射 ACL 条目。

⑧ 拒绝其他 TCP 流量。

⑨ 拒绝其他 UDP 流量。

⑩ 允许其他 IP 流量。

⑪ 在路由器连接外网的接口 Fa0/1 入站方向上应用所定义的 out2inACL。

⑫ 在路由器连接外网的接口 Fa0/1 出站方向上应用所定义的 in2outACL。

⑬ 在内网 10.10.10.2 主机上使用 Telnet 远程登录 200.100.10.2 所触发的反射 ACL。

2.5 基于上下文 ACL 配置

2.5.1 CBAC 简介

基于上下文的访问控制是 Cisco IOS 防火墙安全特性集中的一项特性，它比反射 ACL 具有更多的安全功能。

CBAC 提供 4 项功能：①可以对应用层流量进行状态审查，如发起连接的速率、TCP 序号范围等；②能够根据应用层信息过滤流量；③通过进行流量审查等，可以检测某些类型的 DoS 攻击；④能实时生成警告、审查跟踪信息。

CBAC 工作过程与反射 ACL 很相似。如图 2-12 所示，如果在内网到外网的接口上配置 CBAC 审查流出内网的流量，则当流量通过审查时，将触发建立一个临时的从外网到内网入口 ACL 条目，允许对应该连接外网到内网的返回流量。同时，CBAC 利用一个状态表，记录所监控(审查)连接的状态信息。在对流量进行 CBAC 审查时，网络设备会检查状态表中是否已经存在该连接。如果不存在该连接，则会在状态表中添加该连接相应的条目；如果连接已经存在，就将对应条目的空闲超时清零。

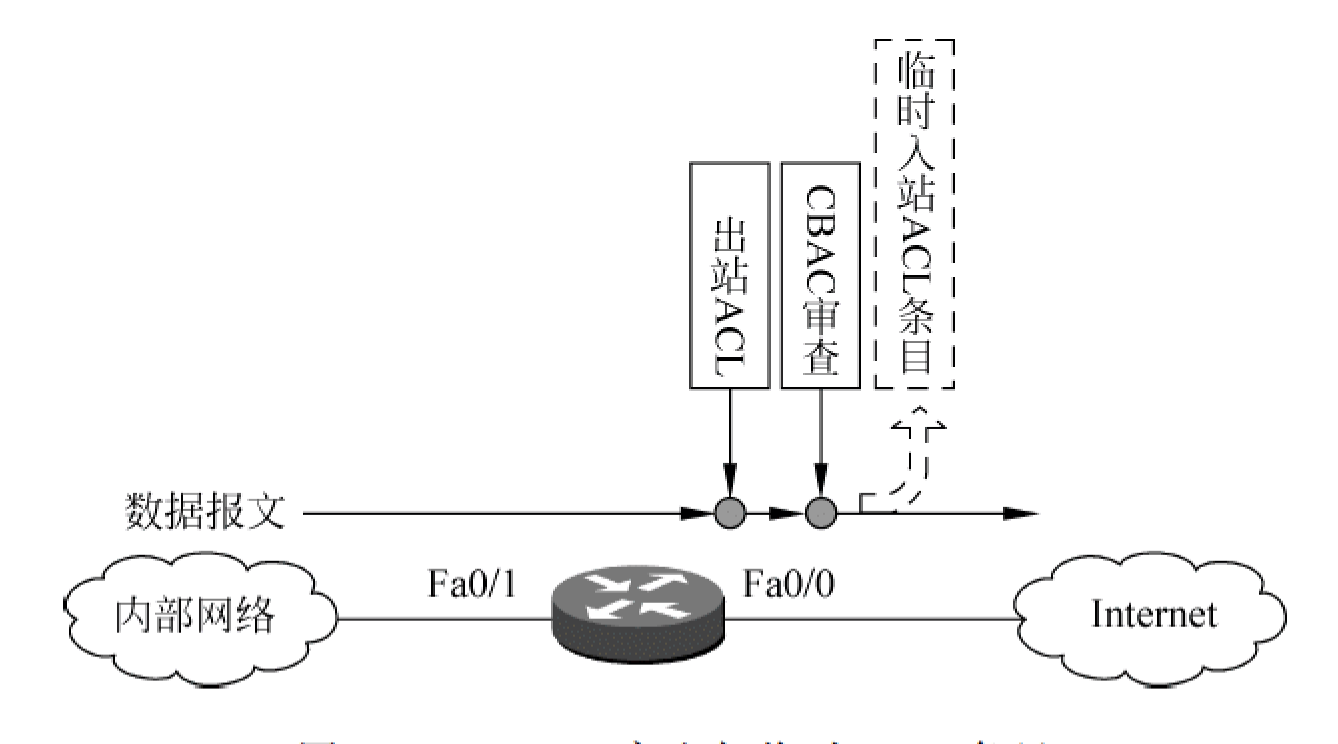


图 2-12 CBAC 审查与临时 ACL 条目

1. TCP流量审查

CBAC审查TCP流量时，检查TCP报文头中的控制位和TCP连接状态。

(1) 如果配置在第1个SYN报文之后的30秒内应建立连接，而在此时间内连接没有建立，则CBAC会从状态表和ACL中删除由第1个SYN报文触发创建的条目。

(2) 如果检查到1个TCP连接空闲超过1小时，则Cisco IOS会从状态表和ACL中删除对应的条目。

(3) 如果检查到TCP报文中有FIN标志，则5秒之后还没有收到后续响应报文，Cisco IOS会从状态表和ACL中删除对应的条目。

(4) 如果收到的TCP报文头中序号与所期望范围不符，则CBAC会丢弃这些数据报文，并会认为有欺骗或DoS发生。

2. UDP流量审查

CBAC审查UDP流量时，与反射ACL处理相同，都是通过估计UDP会话的生命期来进行相应处理。如果配置一个UDP会话空闲时间应为30秒，则如果30秒内该会话上没有UDP流量通过，则Cisco IOS会从状态表和ACL中删除对应的条目。

另外对于DNS的UDP流量，如果配置CBAC审查发出的DNS请求，并且5秒内应能从DNS服务器处获得DNS答复，则当5秒内没有收到答复的情况下，Cisco IOS会从状态表和ACL中删除对应的DNS条目；而一旦在5秒内收到了DNS服务器的答复，则Cisco IOS也会立即从状态表和ACL中删除对应的DNS条目。

3. ICMP流量审查

CBAC对ICMP流量的审查只在12.2(11)版本以后的Cisco IOS中才支持。目前CBAC只能审查几种常见的ICMP消息，如echo、echo-reply、host-unreachable、timestamp-request、timestamp-reply等。CBAC审查ICMP流量时，如果10秒内没有相应的ICMP回应信息返回，则从状态表和ACL中删除对应的连接条目；如果10秒内收到相应的ICMP回应，则检查这些信息，只有被支持的ICMP信息能够通过，其他类型的ICMP信息被丢弃。

4. 附加连接处理与NAT流量处理

(1) 附加连接处理

以FTP连接为例，FTP客户端在使用端口1024与FTP服务器21端口建立起FTP连接后，如果使用被动模式下载文件，则FTP客户端会使用一个新的端口与FTP服务器建立连接。反射ACL由于无法为该附加连接建立相应的动态ACL条目，因此使用反射ACL的网络，就只能使用主动FTP模式的FTP服务。CBAC可以解决这一问题。CBAC会审查FTP客户端与FTP服务器间应用层流量，然后根据FTP流量中的信息分别在状态表、ACL中为附加连接建立相应的条目。

(2) NAT流量处理

在配置了NAT和CBAC的路由器上，对于从外网入站的返回流量，路由器先处理状态表，然后是ACL，最后才是NAT。为了保证状态表中有正确的返回连接条目，同时入站ACL中有正确的返回连接ACL条目，CBAC会在流量从内网到外网时，使用审查功能将内网主机的全局地址动态连接条目加入状态表和ACL。

5. CBAC 对 DoS 攻击的检测

CBAC 可以检测并在一定程度上抵御 DoS 攻击。可以配置 TCP 连接的超时值、TCP 连接数量的阈值，使得 CBAC 审查 TCP 流量时，可以检测到网络中是否存在大量来自单一源地址的 TCP SYN 报文、是否存在指定时间段仍未完成的 TCP 连接。以下为 3 种常用保护内网主机的阈值。

(1) TCP 半连接或未完成的 UDP 会话数。

(2) 一定时间内 TCP 半连接或未完成会话总数。

(3) 每个主机 TCP 半连接总数。

2.5.2　CBAC 配置方法

在 Cisco IOS 中配置 CBAC 的基本步骤如表 2-7 所示。其中，第 1、2 步用于定义和接口上应用过滤流量的 ACL，CBAC 审查产生的动态 ACL 条目会加入到这些 ACL 中；第 3 步用于定义 CBAC 审查规则，该步定义 CBAC 审查哪些协议的流量；第 4 步指定各类协议的超时值，主要用于防范 DoS 攻击；当被审查的网络服务使用了非知名的服务端口来提供服务时，使用第 5 步操作定义端口映射，明确 CBAC 应审查哪些端口；第 6 步定义在哪些流量上应用 CBAC 审查规则；第 7 步对 CBAC 配置进行检查，确保 CBAC 配置正确。

表 2-7　CBAC 基本配置步骤

序　号	操　　作	相 关 命 令	是否必要
步骤 1	定义 ACL	**access-list** 或 **ip access-list**	是
步骤 2	在接口应用 ACL	**ip access-group**	是
步骤 3	定义审查规则	**ip inspect**	是
步骤 4	定义全局超时值，用于防范 DoS	**ip inspect**	可选
步骤 5	定义端口映射，用于审查使用非知名端口提供的服务	**ip port-map**	根据网络服务情况使用
步骤 6	在接口应用审查规则	**ip inspect**	是
步骤 7	检查 CBAC 配置	**show ip inspect** **debug ip inspect**	可选

1. 定义并应用 ACL

在配置 CBAC 时需要注意，只有在相应接口上已经配置应用了扩展 ACL 时，CBAC 才能将审查流量产生的动态 ACL 条目添加到该 ACL 中。

例如图 2-13 中，当为保护内部网络 10.0.0.0/24 的安全而在 Router1 配置 CBAC 时，需要首先保证在 Fa0/0 入站方向上配置有扩展 ACL，这样由 CBAC 审查产生的动态 ACL 才能添加到该扩展 ACL 中。

注意：必须是扩展 ACL 才能使 CBAC 正常工作，因为 CBAC 产生的动态 ACL 条目包含源地址、目的地址、协议类型等扩展 ACL 才有的信息。

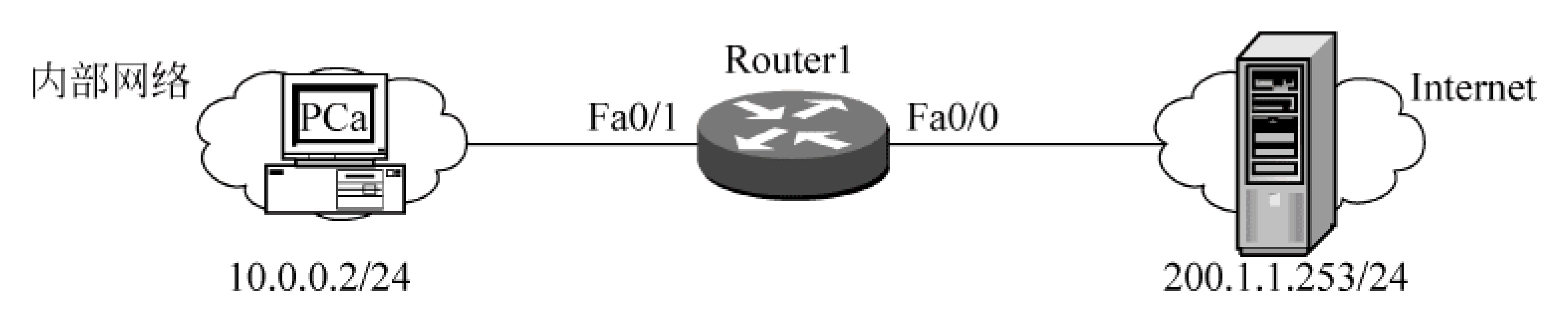


图 2-13　CBAC 配置示例 1

2. 定义及应用审查规则

(1) 定义审查规则

在 Cisco IOS 中,定义审查规则的操作为在全局配置模式下输入:

ip inspect name 审查规则组名 {协议名 | **fragment maximum** 分片最大数} [**alert** { **on** | **off** }] [**audit-trail** { **on** | **off** }] [**timeout** 超时值]

其中,"审查规则组名"参数为该组审查规则在网络设备上的唯一标识。可以通过定义使用同一个审查规则组名的多条审查规则而将多条审查规则绑定在一起。

"协议名"参数定义该审查规则审查哪种协议的流量,该协议必须为 CBAC 支持的协议,如表 2-8 所示。

表 2-8 CBAC 支持的协议

协议名关键字	说　明
cuseeme	CUSeeMe 协议
ftp	文件传输协议
h323	H. 323 协议,例如 MS NetMeeting、Intel Video Phone
http	超文本传输协议
icmp	ICMP 协议
netshow	微软 NetShow 协议
rcmd	远程命令行协议,例如 r-exec、r-login、r-sh
realaudio	Real Audio 协议
rpc	远程过程调用协议
rtsp	Real Time Streaming Protocol
sip	SIP 协议
skinny	Skinny 客户端控制协议,思科专有协议
smtp	简单邮件传输协议
sqlnet	SQL Net Protocol
streamworks	StreamWorks Protocol
tcp	传输控制协议
tftp	TFTP 协议
udp	用户报文协议
vdolive	VDOLive Protocol

fragment 关键字和后面的最大值定义 CBAC 允许会话包含分片的最大数量。

alert 关键字和后面的 on、off 关键字用于定义是否打开警告。

audit-trail 关键字和后面的 on、off 关键字用于定义是否打开审查审计。

timeout 关键字和后面的"超时值"参数用于定义该类会话的超时时间。此处如果未定义超时时间,还可以使用在全局模式下配置的全局超时时间。

(2) 应用审查规则

在 Cisco IOS 中,定义审查规则的操作为在接口配置模式下输入:

ip inspect name 审查规则组名 { **in** | **out** }

其中,"审查规则组名"为前面所定义的审查规则组名。

关键字 in、out 用于指定对接口哪个方向的流量进行审查。

例如，要禁止从 Internet 向内部网络主动发起的 TCP 连接，但允许内部网络向 Internet 主动发起 TCP 连接，则可以在 Router1 上配置如下。

```
Router1(config)# ip access-list extended eacl-out2in                    ①
Router1(config-ext-nacl)# deny tcp any 10.0.0.0 0.0.0.255              ②
Router1(config-ext-nacl)# permit ip any any                             ③
Router1(config-ext-nacl)# exit
Router1(config)# ip inspect name cbac tcp                               ④
Router1(config)# interface fa0/1
Router1(config-if)# ip inspect cbac in                                  ⑤
Router1(config)# interface fa0/0
Router1(config-if)# ip access-group eacl-out2in in                      ⑥
```

以上配置说明如下。

① 创建名为 eacl-out2in 的扩展 ACL，该扩展 ACL 将被应用到 Router1 连接 Internet 的接口入站方向上，用于过滤来自 Internet 的主动 TCP 连接。

② 拒绝所有对内部网络 10.0.0.0/24 的 TCP 流量。由于 CBAC 审查会自动在该 ACL 最前面动态增加 Internet 返回内部网络的 TCP 流量，所以这里使用该命令拒绝所有其他的 TCP 流量。

③ 允许所有 IP 流量，以保证其他流量不受影响。

④ 定义一个组名为 cbac 的审查规则，该审查规则对 TCP 流量进行检查。

⑤ 在 Router1 连接内部网络的入站方向上应用已定义的审查规则 cbac，审查所有内部网络经由 Router1 接口 Fa0/1 进入路由器的 TCP 流量。

⑥ 在 Router1 连接 Internet 的入站方向上应用已定义的扩展 ACL eacl-out2in，过滤所有来自 Internet 的流量。

3. 定义全局超时值及半连接最大值

如前所述，可以定义各类协议的超时值来防御 DoS 攻击。一些常用的超时值定义命令如表 2-9 所示。

表 2-9　常用的超时值定义

ip inspect tcp synwait-time	TCP 会话建立时间①
ip inspect tcp finwait-time	TCP 会话拆除时间②
ip inspect tcp idle-time	TCP 会话空闲时间③
ip inspect udp idle-time	UDP 会话空闲时间④
ip inspect dns-timeout	DNS 查询时间⑤
ip inspect tcp max-incomplete host	单机半连接最大值⑥

注：① 定义 TCP 连接建立，即 3 次握手的最长时间。如果状态表中已有条目超过此时间定义仍未完成 TCP 连接建立过程，则 CBAC 会自动删除状态表中该条目以及 ACL 中动态添加的相应 ACL 条目，该超时值默认为 30 秒；

② 定义开始一个 TCP 会话的拆除过程多长时间后从状态表中删除该 TCP 连接条目，其默认值为 5 秒；

③ 定义状态表中一个 TCP 会话多长时间内没有相应的 TCP 流量经过，则 CBAC 会将其状态表条目和 ACL 中相应条目删除，其默认值为 3600 秒；

④ 定义状态表中一个 UDP 会话多长时间内没有相应的 UDP 流量经过，则 CBAC 会将其状态表条目和 ACL 中相应条目删除，其默认值为 30 秒；

⑤ 定义状态表中一个 DNS 请求多长时间还未收到答复后，CBAC 会将其状态表条目和 ACL 中相应条目删除，其默认值为 5 秒；

⑥ 定义每台主机的最大半连接会话数，范围为 1～4294967295。

4. 定义端口映射

CBAC 审查各类网络应用协议时，默认按照此类网络应用协议的知名端口对其流量进行审查。当实际网络中的网络服务使用了非知名端口提供网络服务时，为保证 CBAC 工作正常，需要配置端口映射，以使得 CBAC 能够正确的审查网络应用协议。

在 Cisco IOS 中，定义端口映射的操作为在全局配置模式下输入：

ip port-map 网络服务名 **port** 端口号 ［标准 **ACL** 名］

其中，"网络服务名"参数用于指定哪类网络服务使用了非知名端口。

"端口号"参数用于定义该网络服务使用了什么端口。

可选参数"标准 ACL 名"用于指定哪些网络中的主机在提供该类网络服务时使用了所定义的非知名端口。

配置完端口映射后，可以在特权模式下使用 show ip port-map 命令来查看端口映射配置情况。该命令语法如下。

show ip port-map ［｛网络服务名｜ **port** 端口号｝］

该命令不带任何参数，则显示各类网络服务在 Cisco IOS 中默认对应的端口。

该命令带网络服务名参数，则显示指定网络服务的系统默认和用户使用端口映射自定义的端口。

该命令带 port 关键字和"端口号"参数，则显示系统中指定端口号对应的网络服务。

show ip port-map 命令输出结果如下。

```
Router1(config)#ip port-map http port 80
Router1(config)#exit
Router1# show ip port-map http
Default mapping: http          port 8080          user defined
Default mapping: http          port 80            system defined
Default mapping: http          port 8090          user defined
Router1# show ip port-map port 80
Default mapping: http          port 80            system defined
Router1# show ip port-map
Default mapping: dns           port 53            system defined
…
Default mapping: http          port 80            system defined
```

5. 检查 CBAC 配置

在 Cisco IOS 中，可以使用 3 种方法检查 CBAC 的配置是否符合要求：show 命令、debug 命令、警告和审计。

(1) show 命令

在 Cisco IOS 中可以在特权模式下输入以下命令来查看 CBAC 审查执行情况。

show ip inspect ｛ **sessions** ｜ **stat** ｝

其中，使用 sessions 参数，将显示当前状态表中的会话条目。

使用 stat 参数，将显示到目前为止，CBAC 状态表会话条目的统计信息。

show　ip　inspect 命令的输出结果如下。

```
Router1# show  ip  inspect  sessions
Established Sessions
Session 640008CC (10.0.0.254:0)=>(0.0.0.0:0) icmp SIS_OPEN                    ①
Router1# show  ip  inspect  stat
Interfaces configured for inspection 1                                         ②
Session creations since subsystem startup or last reset 14                     ③
Current session counts (estab/half-open/terminating) [0:0:0]                   ④
Maxever session counts (estab/half-open/terminating) [0:1:0]                   ⑤
Last session created 00:00:34
Last statistic reset never
Last session creation rate 1
Last half-open session total 0
```

以上输出结果说明如下。

① 当前状态表中有 1 条会话条目，该条目为主机 10.0.0.254 发出 ICMP 请求触发的条目。

② 截至命令执行时刻，已在 1 个接口上配置了 CBAC 审查。

③ 自从上次系统 CBAC 启动或重新设置开始到该命令执行时刻，状态表中共记录过 14 条会话。

④ 当前已建立、半连接、终止的会话条目数。

⑤ 已建立、半连接、终止的最大会话条目数。

(2) debug 命令

在 Cisco IOS 中，可以在特权模式下输入以下命令来跟踪 CBAC 审查执行情况。

```
debug  ip  inspect  协议名
```

参数“协议名”用于定义只显示被审查的 ICMP 流量。

该命令输出结果如下。

```
Router1# debug  ip  inspect  icmp                                              ①
INSPECT ICMP Inspection debugging is on
Router1#
* Mar  1 05:50:11.306: CBAC ICMP: sis 640008CC pak 63C1BCCC SIS_CLOSED         ②
ICMP packet (10.0.0.254:0) => (0.0.0.0:0) datalen 72
* Mar  1 05:50:11.446: CBAC* ICMP: sis 640008CC pak 63E66810 SIS_OPENING       ③
ICMP packet (10.0.0.254:0) <= (0.0.0.0:0) datalen 72
```

以上输出结果说明如下。

① 打开 ICMP 协议的 CBAC 审查跟踪。

② 在 10.0.0.254 上执行 ping 命令后，CBAC 的审查信息。

③ 收到返回给 10.0.0.254 的 ICMP 响应后，CBAC 的审查信息。

2.6 模拟公司分支机构网络边界安全访问控制列表配置示例

模拟公司分支机构 A-1 网络边界使用 Cisco 3800 系列路由器，分支机构 C-2 网络边界使用 Cisco 2800 系列路由器。为防御可能来自 Internet 的网络攻击，可分别参照本部分方案 1、方案 2 配置所示，配置访问控制列表，实现 2.1.2 小节安全配置方案。

注意：此处的 ACL 配置未考虑实施 NAT、VPN 等配置要求，关于 NAT、VPN 部分可参阅本书其他有关章节。

分支机构 A-1 网络拓扑结构如图 2-14 所示。

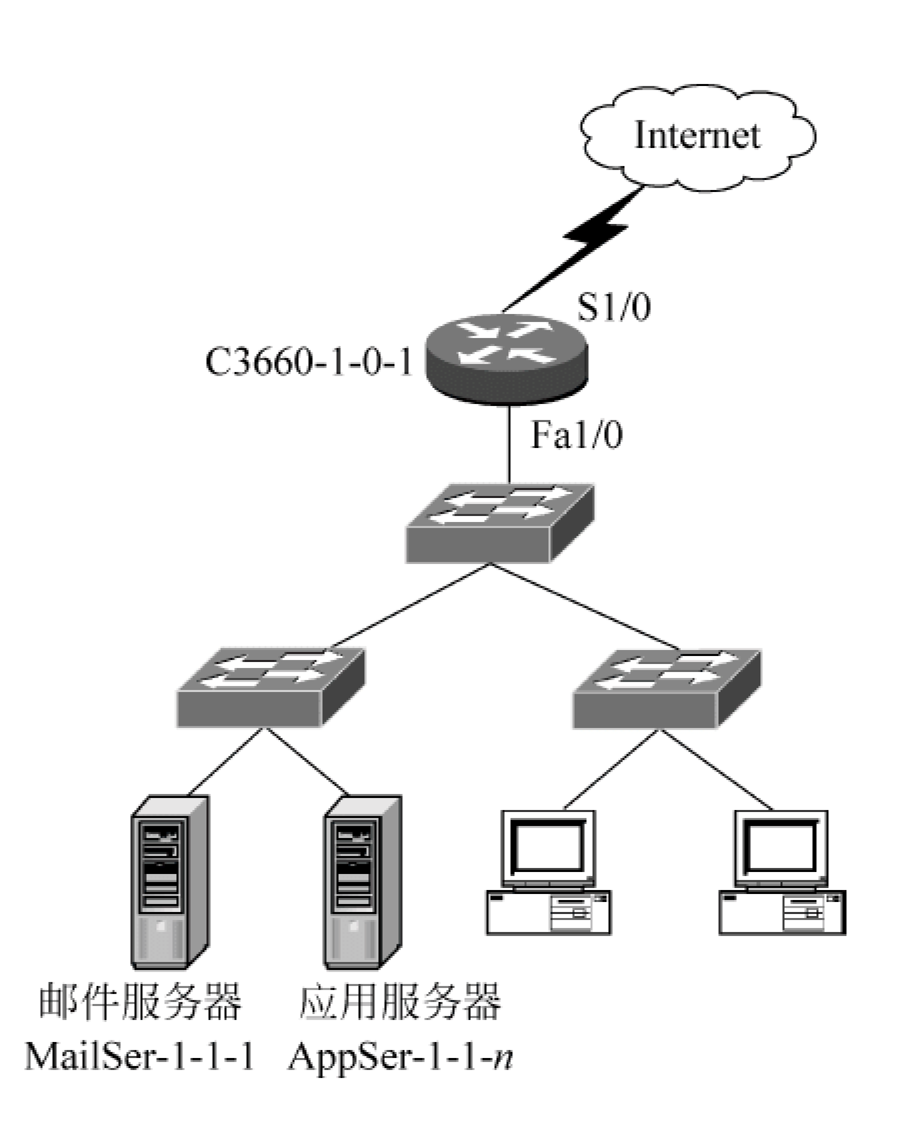


图 2-14　分支机构 A-1 网络拓扑示意图

总公司及分支机构 IP 地址分配情况如表 2-10 所示。分支机构网络内 IP 地址分配情况如表 2-11 所示。其中各分支机构最后 16 个 IP 地址，分别作为网络设备管理地址和网络服务器 IP 地址。

表 2-10　模拟公司 IP 地址分配

机　构	IP　网　络	可用 IP 地址数量
总公司	200.100.8.0/22	1022
分公司 1	200.100.12.0/24	254
分公司 2	200.100.13.0/24	254
分支 A-1	200.100.14.0/25	126
分支 A-2	200.100.14.128/26	62
分支 A-3	200.100.14.192/26	62
分支 B-1	200.100.15.0/26	62
分支 B-2	200.100.15.64/26	62
分支 C-1	200.100.15.128/27	30
分支 C-2	200.100.15.160/27	30
串行链路 1	200.100.15.192/30	2
串行链路 2	200.100.15.196/30	2
串行链路 3	200.100.15.200/30	2
串行链路 4	200.100.15.204/30	2
串行链路 5	200.100.15.208/30	2
串行链路 6	200.100.15.212/30	2
串行链路 7	200.100.15.216/30	2
串行链路 8	200.100.15.220/30	2
串行链路 9	200.100.15.224/30	2

表 2-11　分支机构网络 IP 地址分配

设　　备	IP　地　址
分支 A-1 邮件服务器地址	200.100.14.117/29
分支 A-1 应用服务器地址	200.100.14.113～200.100.14.116/29
分支 A-1 网络设备管理地址	200.100.14.121～200.100.14.126/29
分支 C-2 邮件服务器地址	200.100.15.181/29
分支 C-2 应用服务器地址	200.100.15.177～200.100.15.180/29
分支 C-2 网络设备管理地址	200.100.15.185～200.100.15.189/29

方案 1

(1) 在 C3660-1-0-1 S1/1 接口入站方向上配置扩展 ACL。

- 拒绝 bogon 主机对分支机构网络的 IP 流量。
- 配置定时 ACL 条目，允许到应用服务器指定端口的流量。
- 允许到邮件服务器的邮件通信流量。
- 允许到内网网络设备的 SSH 流量。
- 允许从 Internet 到内网网络设备和服务器的 ICMP 流量。
- 拒绝所有来自 Internet 的 TCP、UDP、ICMP 流量。
- 允许来自 Internet IP 流量。

(2) 在 C3660-1-0-1 S1/0 接口入站方向上配置 CBAC 条目 cbac，允许从 Internet 返回的 TCP、UDP、ICMP 流量。

(3) 在 C3660-1-0-1 连接分支网络的各子接口入站方向配置拒绝所有 TCP 和 UDP 1524、27444、27665、16660、65000、31335 端口，IRC 服务的 TCP 6665～6669 端口和木马常用端口流量。

(4) 在 C3660-1-0-1 连接分支网络的各子接口入站方向配置 CBAC 审查 TCP、UDP、ICMP 流量，与 S1/0 接口入站方向上扩展 ACL 条目配合，拒绝所有 Internet 到分支机构网络内除服务器外其他主机的主动连接。

(5) 在分支网络所有网络设备 VTY 线路上配置标准 ACL，拒绝 bogon 地址主机但允许其他主机使用 SSH 远程登录管理网络设备。

方案 1 配置如下。

```
ip  inspect  name  cbac tcp                                    ①
ip  inspect  name  cbac  udp  timeout  30
ip  inspect  name  cbac  icmp                                  ②
此处省略部分显示...
interface Loopback0
ip  address  200.100.14.114  255.255.255.255
此处省略部分显示...
interface FastEthernet0/0.10
此处省略部分显示...
ip  access-group  eacl-in2out  in                              ③
ip  inspect  cbac  in                                          ④
interface FastEthernet0/0.20
```

```
此处省略部分显示...
ip  access-group  eacl-in2out  in
ip  inspect  cbac  in
此处省略部分显示...
interface Serial1/0
ip  address  200.100.15.197  255.255.255.252
ip  access-group  eacl-out2in in                                          ⑤
此处省略部分显示...
ip  access-list  standard  sacl-ssh                                       ⑥
deny   10.0.0.0  0.255.255.255
deny   14.0.0.0  0.255.255.255
此处省略部分显示...
permit  any
!
ip  access-list  extended  eacl-in2out
deny   tcp  any  any  eq  33270                                           ⑦
deny   tcp  any  eq  33270  any
deny   tcp  any  any  eq  39168
deny   tcp  any  eq  39168  any
deny   udp  any  eq  1524  any
deny   udp  any  any  eq  1524
此处省略部分显示...
permit  ip  any  any                                                      ⑧
ip  access-list  extended  eacl-out2in
deny   ip  0.0.0.0  1.255.255.255 any                                     ⑨
deny   ip  2.0.0.0  0.255.255.255 any
deny   ip  5.0.0.0  0.255.255.255 any
此处省略部分显示...
deny   ip  224.0.0.0  31.255.255.255  any
deny   ip  200.100.14.0  0.0.0.127  any                                   ⑩
permit  tcp  any  200.100.14.112  0.0.0.7  eq  22                         ⑪
permit  tcp  any  host  200.100.14.126  eq  smtp                          ⑫
permit  tcp  any  host  200.100.14.126  eq  pop3                          ⑬
permit  tcp  any  200.100.14.112  0.0.0.7  range  3000  3010  time-range  wkday   ⑭
permit  icmp  any  200.100.14.112  0.0.0.15                               ⑮
deny   tcp  any  any                                                      ⑯
deny   udp  any  any
deny   icmp  any  any                                                     ⑰
permit  ip  any  any                                                      ⑱
此处省略部分显示...
line vty 0 4
access-class  sacl-ssh  in                                                ⑲
此处省略部分显示...
time-range  wkday
periodic  weekdays  9:00  to  17:00                                       ⑳
```

方案 1 配置说明如下。

①～② 配置对 TCP、UDP、ICMP 流量进行审查，这 3 条命令配合访问控制列表 eacl-out2in 实现仅允许分支机构网络到 Internet 的 TCP、UDP、ICMP 连接，禁止 Internet 到

分支机构网络的主动 TCP、UDP、ICMP 连接。

③ 在边界路由器连接分支机构网络的各子接口上，配置禁止疑为 DDoS 攻击的流量入站，防御分支机构网络内主机被攻陷后主动向 Internet 外恶意用户发起的 DDoS 连接。

④ 在边界路由器连接分支机构网络的各子接口上，配置对入站 TCP、UDP、ICMP 流量进行审查。

⑤ 在边界路由器连接 Internet 的接口上，应用对入站流量进行过滤的访问控制列表 eacl-out2in。

⑥ 该命令定义用于限制 bogon 主机使用 SSH 远程访问该边界路由器的标准 ACL，用于防御使用假冒 IP 地址对分支机构网络发动的攻击。

⑦～⑧ 定义访问控制列表 eacl-in2out，禁止可能被 DDoS 攻击利用访问流量。

⑨～⑩ 该命令定义禁止 bogon 主机访问分支机构网络的 ACL 条目。

⑪ 该命令定义允许使用 SSH 远程管理各网络设备的 ACL 条目。

⑫～⑬ 该两条命令定义允许访问分支机构邮件服务器的 ACL 条目。

⑭ 该命令用于定义允许 Internet 在指定时间访问分支机构应用服务器 TCP 3000～3010 端口上提供的网络应用服务。

⑮ 该命令用于允许使用 ping 从 Internet 检查分支机构网络设备、服务器的连通性。

⑯～⑰ 这 3 条命令与审查命令配合，禁止 Internet 到分支机构网络主动 TCP、UDP、ICMP 连接。

⑱ 为保证路由协议等能正常工作，允许所有其他 IP 流量。

⑲ 在该边界路由器远程访问线路上应用禁止 bogon 主机访问的标准 ACL。

⑳ 为定时 ACL 条目定义的时间段 wkday，该时间段为每周一至周五的早 9：00 到下午 5：00。

方案 2

(1) 在 C2800-2-0-1 S1/1 接口入站方向上配置扩展 ACL。

- 拒绝 bogon 主机对分支机构网络的 IP 流量。
- 配置定时 ACL 条目，允许到应用服务器指定端口的流量。
- 允许到邮件服务器的邮件通信流量。
- 允许到内网网络设备的 SSH 流量。
- 允许从 Internet 到内网网络设备和服务器的 ICMP 流量。
- 允许所有来自 Internet 的 TCP、UDP、ICMP 返回流量。
- 拒绝所有来自 Internet 的 TCP、UDP、ICMP 流量。
- 允许来自 Internet IP 流量。

(2) 在 C2600-2-0-1 Fa0/1 接口入站方向上配置扩展 ACL。

- 允许 TCP、UDP、ICMP 流量的反射 ACL。
- 拒绝所有 TCP 和 UDP 1524、27444、27665、16660、65000、31335 端口，IRC 服务的 TCP 6665～6669 端口和木马常用端口流量。
- 允许其他所有 IP 流量。

(3) 在分支网络所有网络设备 VTY 线路上配置标准 ACL，拒绝 bogon 地址主机但

允许其他主机使用 SSH 远程登录管理网络设备。

方案 2 配置如下。

```
interface Loopback0
ip  address  200.100.14.114  255.255.255.255
此处省略部分显示...
interface FastEthernet0/0.10
此处省略部分显示...
ip  access-group  eacl-in2out  in
interface FastEthernet0/0.20
此处省略部分显示...
ip  access-group  eacl-in2out  in
此处省略部分显示...
interface Serial1/0
ip  address  200.100.15.197  255.255.255.252
ip  access-group  eacl-out2in in
此处省略部分显示...
ip  access-list  standard  sacl-ssh
deny   10.0.0.0  0.255.255.255
deny   14.0.0.0  0.255.255.255
此处省略部分显示...
permit  any
!
ip  access-list  extended  eacl-in2out
deny   tcp  any  any  eq  33270
deny   tcp  any  eq  33270  any
deny   tcp  any  any  eq  39168
deny   tcp  any  eq  39168  any
deny   udp  any  eq  1524  any
deny   udp  any  any  eq  1524
此处省略部分显示...
permit  tcp  any  any  reflect  rf-tcp        ①
permit  udp  any  any  reflect  rf-udp
permit  icmp  any  any  reflect  rf-icmp      ②
permit  ip  any  any
ip  access-list  extended  eacl-out2in
deny   ip  0.0.0.0  1.255.255.255 any
deny   ip  2.0.0.0  0.255.255.255 any
deny   ip  5.0.0.0  0.255.255.255 any
此处省略部分显示...
deny   ip  224.0.0.0  31.255.255.255  any
deny   ip  200.100.14.0  0.0.0.127  any
evaluate  rf-tcp                              ③
evaluate  rf-udp
evaluate  rf-icmp                             ④
permit  tcp  any  200.100.14.112  0.0.0.7  eq  22
permit  tcp  any  host  200.100.14.126  eq  smtp
permit  tcp  any  host  200.100.14.126  eq  pop3
permit  tcp  any  200.100.14.112  0.0.0.7  range  3000  3010  time-range  wkday
```

```
permit  icmp  any  200.100.14.112  0.0.0.15
deny   tcp  any  any
deny   udp  any  any
deny   icmp  any  any
permit  ip  any  any
此处省略部分显示...
line vty 0 4
access-class  sacl-ssh  in
此处省略部分显示...
time-range  wkday
periodic  weekdays  9:00  to  17:00
```

方案 2 配置说明如下。

①～② 为产生反射 ACL 定义的允许内网网络到 Internet 的 TCP、UDP、ICMP 流量。

③～④ 引用反射 ACL，允许 Internet 返回内网网络的 TCP、UDP、ICMP 流量。

2.7　小结

网络设备使用 ACL 实现流量过滤功能。ACL 类型分为无状态 ACL、有状态 ACL 和基于上下文 ACL 3 种。根据功能划分，无状态 ACL 分为基本 ACL、扩展 ACL、基于时间的 ACL 等。ACL 的基本配置步骤分为两步：定义 ACL、应用 ACL。有状态 ACL 可以根据被允许的流量，动态产生允许相应反向流量的 ACL 条目。基于上下文的 ACL 也可以根据被审查流量的配置，动态产生反向 ACL 条目。

2.8　习题

1. 下面的 ACL 应用在图 2-15 中哪个位置最为恰当？（　　）

```
permit  tcp  host  10.0.0.1  eq  80  any
deny  tcp  any  any
permit  ip  any  any
```

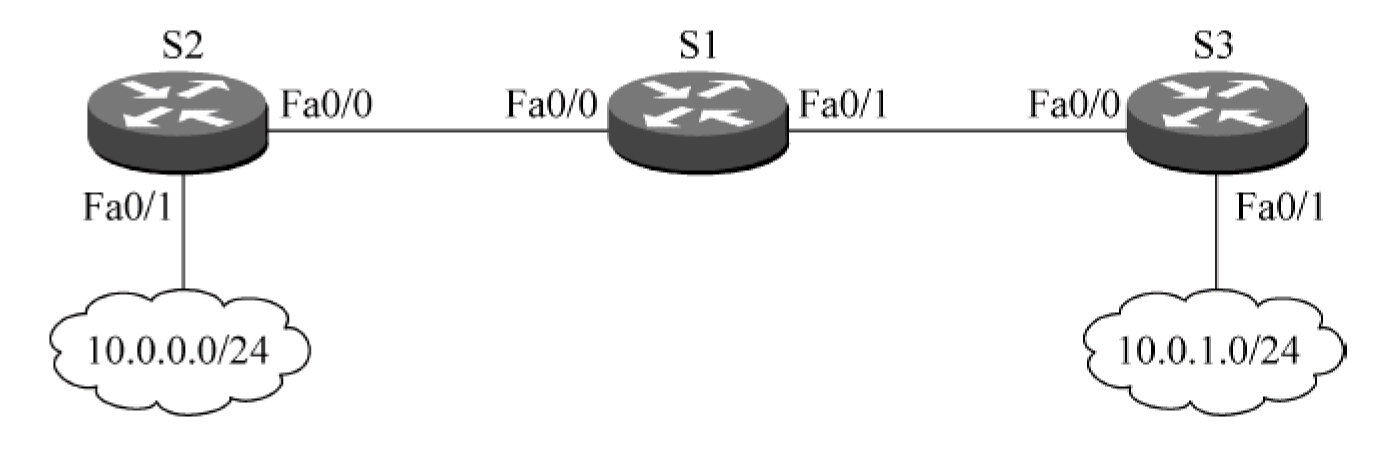


图 2-15　题 1 图

A. S2 接口 Fa0/1 的入站方向

B. S2 接口 Fa0/1 的出站方向

C. S2 接口 Fa0/0 的入站方向

D. S2 接口 Fa0/0 的出站方向
E. S1 接口 Fa0/1 的入站方向
F. S1 接口 Fa0/1 的出站方向
G. S1 接口 Fa0/0 的入站方向
H. S1 接口 Fa0/0 的出站方向
I. S3 接口 Fa0/0 的入站方向
J. S3 接口 Fa0/0 的出站方向
K. S3 接口 Fa0/1 的入站方向
L. S3 接口 Fa0/1 的出站方向

2. 判断题：下面的 ACL 可以用于禁止来自 10.0.0.0/24 的 IP 流量，但允许来自其他网络的流量。

```
ip access-list standard sacl-test
deny    10.0.0.0   0.255.255.255
```

3. 判断题：对于匹配了带有 established 关键字 ACL 条目的流量，路由器会检查是否存在对应的会话连接记录。

4. 简述使用 ACL 防御 IP 地址欺骗攻击的方法。

5. 简述配置 CBAC 的基本步骤。

2.9 实训

2.9.1 无状态 ACL 配置

1. 实训组织

实训学时：100 分钟。

学生分组：2 人/组。

2. 实训目的

(1) 通过实训，熟练掌握标准 ACL、扩展 ACL、定时 ACL 和分片 ACL 的配置应用方法。

(2) 加深对 TCP、UDP 等协议工作原理的理解。

(3) 理解几类典型网络攻击手段的工作原理，掌握使用标准 ACL、扩展 ACL、定时 ACL 和分片 ACL 防范攻击的方法。

3. 实训环境

(1) 安装有 Windows 系统、Wireshark 软件和 HTTP、FTP 服务器软件的 PC，每组 3 台。

(2) Cisco 二层交换机，每组 1 台。

(3) Cisco 路由器(建议 2600 系列或 2800 系列)，每组 1 台。

(4) UTP 直通电缆，每组 3 条。

(5) UTP 交叉电缆，每组 1 条。

(6) Console 电缆，每组 2 条。

注意保持所有的交换机、路由器为出厂配置。

4. 实训准备

按照图 2-16 所示搭建简化的模拟公司分支机构网络，并按照 2.6 节方案 1 中 IP 地址分配情况，配置网络连接和路由，注意为交换机 C2960-9-0-1 和路由器 C2600-9-0-1 配置管理地址，交换机 C2960-9-0-1 的管理 VLAN 号为 99，网络内服务器所在 VLAN 编号为 10，其他 PC 所在 VLAN 编号为 20。

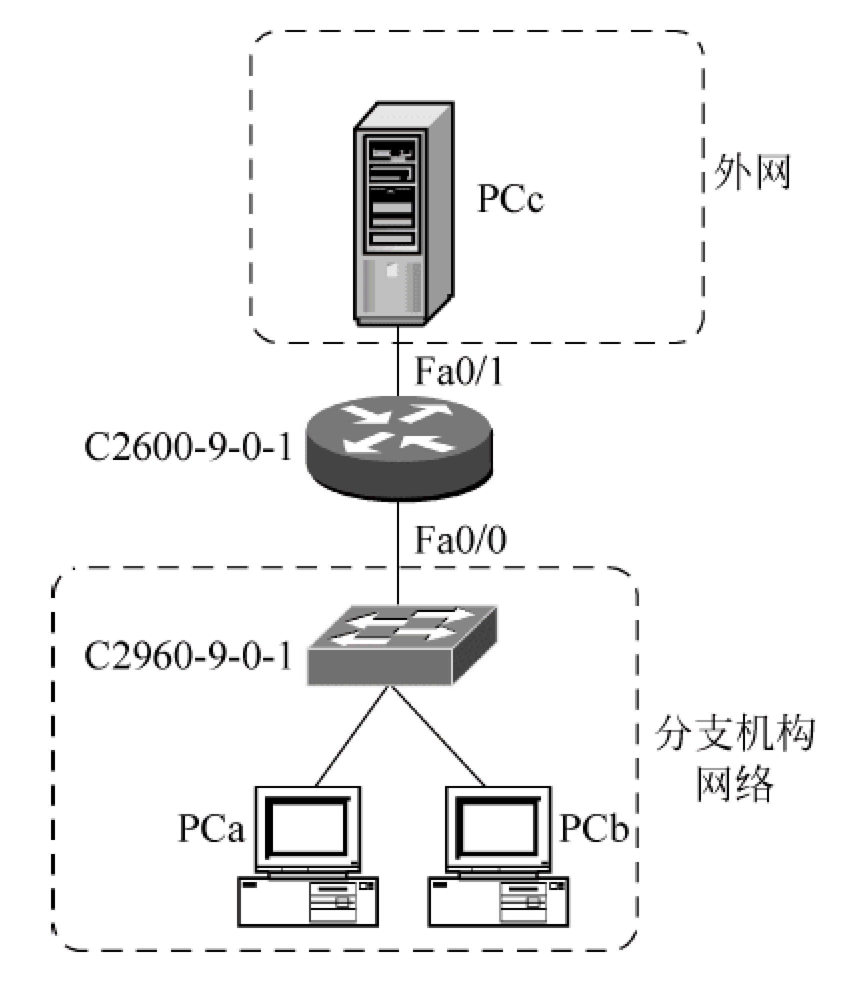


图 2-16　无状态 ACL 配置实训网络拓扑

本实训为简化检测对实训环境的要求，采用 HTTP、FTP 服务替代模拟公司方案中的邮件服务和应用服务。实训前，在 PCc、PCb 上启动 HTTP、FTP 服务程序，并检测 PCa、PCc 均能访问 PCc、PCb 上的 HTTP、FTP 服务。

5. 实训内容

(1) 配置标准 ACL，拒绝所有 bogon 主机使用 Telnet 远程登录路由器和内网交换机。

(2) 配置扩展 ACL 条目，允许所有内网对外网主动 TCP 连接，拒绝所有 Internet 对内网的 TCP 连接请求。

(3) 配置定时 ACL 条目，允许 Internet 在指定时间段访问内网 HTTP、FTP 服务器。

6. 实训指导

进行实训前，先在 PCa 上分别 ping 路由器、交换机管理地址以及 PCc 来测试网络连通性。

(1) 配置标准 ACL，拒绝 bogon 主机攻击。在路由器远程访问线路接口的恰当方向上配置标准 ACL，拒绝来自 bogon 主机的访问。配置步骤如下。

```
C2600-9-0-1(config)# ip   access-list   standard   sacl-telnet
C2600-9-0-1(config-std-nacl)# deny   0.0.0.0   1.255.255.255
C2600-9-0-1(config-std-nacl)# deny   2.0.0.0   0.255.255.255
C2600-9-0-1(config-std-nacl)# deny   5.0.0.0   0.255.255.255
C2600-9-0-1(config-std-nacl)# deny   10.0.0.0   0.255.255.255
C2600-9-0-1(config-std-nacl)# deny   14.0.0.0   0.255.255.255
C2600-9-0-1(config-std-nacl)# deny   23.0.0.0   0.255.255.255
C2600-9-0-1(config-std-nacl)# deny   27.0.0.0   0.255.255.255
C2600-9-0-1(config-std-nacl)# deny   31.0.0.0   0.255.255.255
C2600-9-0-1(config-std-nacl)# deny   36.0.0.0   1.255.255.255
C2600-9-0-1(config-std-nacl)# deny   39.0.0.0   0.255.255.255
C2600-9-0-1(config-std-nacl)# deny   42.0.0.0   0.255.255.255
此处省略部分配置...
C2600-9-0-1(config-std-nacl)# permit   any
C2600-9-0-1(config-std-nacl)# exit
C2600-9-0-1(config)# line   vty   0   4
```

```
C2600-9-0-1(config-line)# access-class sacl-telnet in
C2600-9-0-1(config-line)# password 123
C2600-9-0-1(config-line)# login
C2600-9-0-1(config-line)# exit
```

配置完成后,在模拟外网主机 PCc 上运行 Telnet 程序,测试能否远程登录路由器。

修改模拟外网主机的 IP 地址为 bogon 地址,测试能否远程登录路由器。

参照以上操作,在交换机远程访问线路接口的恰当方向上配置标准 ACL,拒绝来自 bogon 主机的访问。

配置完成后,在模拟外网主机上运行 Telnet 程序,测试能否远程登录交换机。

修改模拟外网主机的 IP 地址为 bogon 地址,测试能否远程登录交换机。

(2) 主动 TCP 连接条目配置。在路由器远程访问线路接口的恰当方向上配置扩展 ACL,允许来自 Internet 的已建立 TCP 连接,拒绝其他 TCP 流量。配置步骤如下。

```
C2600-9-0-1(config)# ip access-list extended eacl-out2in
C2600-9-0-1(config-ext-nacl)# permit tcp any any established
C2600-9-0-1(config-ext-nacl)# deny tcp any any
C2600-9-0-1(config-ext-nacl)# permit ip any any
C2600-9-0-1(config-ext-nacl)# exit
C2600-9-0-1(config)# interface fa0/1
C2600-9-0-1(config-if)# ip access-group eacl-out2in in
```

配置完成后,在模拟外网主机上运行浏览器程序,测试能否访问内网的 HTTP、FTP 服务器。

测试能否在模拟内网主机上运行浏览器程序,访问外网的 HTTP、FTP 服务器。

使用 show ip access-lists 命令检查 ACL 匹配情况。

(3) 定时 ACL 配置。在路由器远程访问线路接口的恰当方向,按恰当顺序配置定时 ACL 条目,允许来自 Internet 对内网服务器的主动 TCP 连接。配置步骤如下。

```
C2600-9-0-1(config)# time-range wkday
C2600-9-0-1(config-time-range)# periodic weekdays 9:00 to 17:00
C2600-9-0-1(config)# ip access-list extended eacl-out2in
C2600-9-0-1(config-ext-nacl)# 15 permit tcp any 200.100.14.120 0.0.0.7 eq 80
time-range wkday
C2600-9-0-1(config-ext-nacl)# 16 permit tcp any 200.100.14.120 0.0.0.7 eq 21
time-range wkday
C2600-9-0-1(config-ext-nacl)# 17 permit tcp any 200.100.14.120 0.0.0.7 eq 20
time-range wkday
C2600-9-0-1(config-ext-nacl)# end
C2600-9-0-1# show clock
12:54:06.523 UTC Thu Sep 10 2009
C2600-9-0-1# show ip access-lists
此处省略部分显示...
15 permit tcp any 200.100.14.120 0.0.0.7 eq 80 time-range wkday (active)
16 permit tcp any 200.100.14.120 0.0.0.7 eq 21 time-range wkday (active)
17 permit tcp any 200.100.14.120 0.0.0.7 eq 20 time-range wkday (active)
C2600-9-0-1# clock set 05:00:00 Sep 10 2009
```

```
C2600-9-0-1# show  clock
05:00:04.767 UTC Thu Sep 10 2009
C2600-9-0-1# show  ip  access-lists
此处省略部分显示...
15  permit  tcp  any  200.100.14.120  0.0.0.7  eq  80  time-range  wkday (inactive)
16  permit  tcp  any  200.100.14.120  0.0.0.7  eq  21  time-range  wkday (inactive)
17  permit  tcp  any  200.100.14.120  0.0.0.7  eq  20  time-range  wkday (inactive)
```

配置完成后，使用 clock 命令修改路由器的时钟，从模拟外网的主机上运行浏览器程序，测试路由器不同时间段，能否访问内网的 HTTP 服务器。

注意：该例在定义 ACL 条目时，在命令前指定 ACL 条目序号以插入 ACL 条目。

7. 实训报告

1. 网络连接情况

接口	IP/网络前缀	VLAN 编号	网关地址
路由器接口 Fa0/0	________	/	/
路由器子接口	________	99	/
路由器子接口	________	10	/
路由器子接口	________	20	/
路由器管理地址	________	____	____
交换机管理地址	________	____	____
PCa	________	____	____
PCb	________	____	____
PCc	________	____	____

2. 标准 ACL sacl-telnet 所有条目及含义

ACL 条目	命令说明

3. 回答问题

如果在路由器 Fa0/1 接口配置禁止来自 Internet 的主动 TCP 连接 ACL 条目，但允许来自 Internet 到达网络设备的 Telnet 访问，则应如何配置 ACL？

ACL 条目	命令说明

续表

4. 回答问题 如果分支机构网络中的网络设备、服务器上的 Telnet 服务只在周末才允许来自 Internet 的主机访问，其他时刻仅允许分支机构网络内部主机访问，则在前述 ACL 条目基础上，应如何配置实现该功能的 ACL 条目？	
ACL 条目	命令说明
应用该 ACL 的命令是什么？	
应用 ACL 的命令	命令说明

2.9.2 有状态及基于上下文 ACL 配置

1. 实训组织

实训学时：100 分钟。

学生分组：2 人/组。

2. 实训目的

（1）通过实训，熟练掌握反射 ACL、CBAC 的配置应用方法。

（2）加深对 TCP、UDP 等协议工作原理的理解。

（3）理解几类典型网络攻击手段的工作原理，掌握使用反射 ACL、CBAC 防范各类网络攻击的方法。

3. 实训环境

（1）安装有 Windows 系统、Wireshark 软件和 HTTP、FTP 服务器软件及网络攻击软件的 PC，每组 3 台。

（2）Cisco 二层交换机，每组 1 台。

（3）Cisco 路由器（建议 3600 系列或 3800 系列），每组 1 台。

（4）UTP 直通电缆，每组 3 条。

（5）UTP 交叉电缆，每组 1 条。

（6）Console 电缆，每组 2 条。

注意保持所有的交换机、路由器为出厂配置。

4. 实训准备

按照图 2-17 所示搭建简化的模拟公司分支机构网络，并按照 2.6 节方案 1 中 IP 地址分配情况，配置网络连接和路由，注意为交换机 C2960-9-0-1 和路由器 C3600-9-0-1 配置管理地址，交换机 C2960-9-0-1 的管理 VLAN 号为 99，网络内服务器所在 VLAN 编号为 10，其他 PC 所在 VLAN 编号为 20。

本实训为简化检测对实训环境的要求，采用 HTTP、FTP 服务替代模拟公司方案中的邮件服务和应用服务。实训前，在 PCc、PCb 上启动 HTTP、FTP 服务程序，并检测 PCa、PCc 均能访问 PCc、PCb 上的 HTTP、FTP 服务。

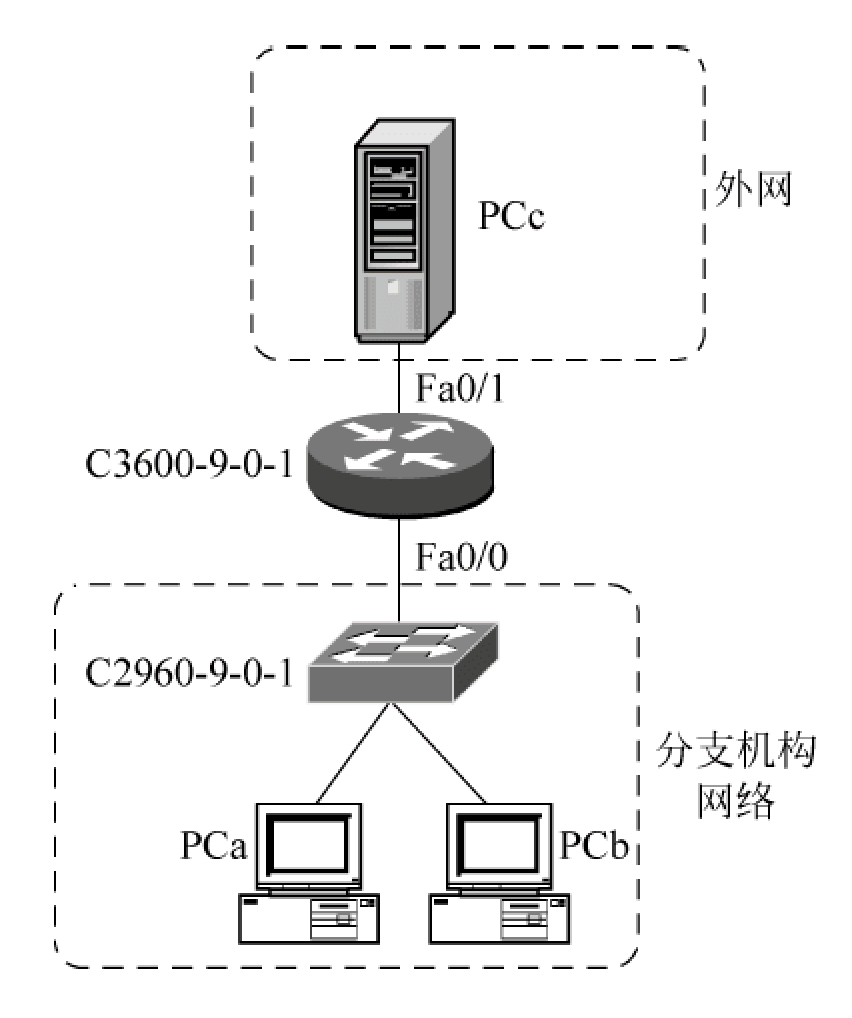


图 2-17 有状态 ACL 实训配置网络拓扑

5. 实训内容

（1）配置反射 ACL，禁止外网对内网的主动 TCP、UDP、ICMP 连接。

（2）配置 CBAC，禁止外网对内网的主动 TCP、UDP、ICMP 连接。

6. 实训指导

进行实训前，先在 PCa 上分别 ping 路由器、交换机管理地址以及 PCc 来测试网络连通性。

注意：本部分实训为简化配置，在路由器 Fa0/1 接口配置应用反射 ACL、CBAC，与 2.6 节方案 1、方案 2 位置不同。

（1）反射 ACL 配置，禁止外网对内网的主动 TCP、UDP、ICMP 连接。根据 2.6 节方案 2，在路由器接口的恰当方向上配置反射 ACL，禁止外网对内网的主动 TCP、UDP、ICMP 连接。配置步骤如下。

```
C3660-1-0-1(config)# ip access-list extended eacl- in2out
C3660-9-0-1(config-ext-nacl)# permit tcp any any reflect rf-tcp
C3660-9-0-1(config-ext-nacl)# permit udp any any reflect rf-udp
C3660-9-0-1(config-ext-nacl)# permit icmp any any reflect rf-icmp
C3660-9-0-1(config-ext-nacl)# exit
C3660-1-0-1(config)# interface fa0/1
C3660-1-0-1(config-if)# ip access-group eacl-in2out out
C3660-1-0-1(config-if)# exit
C3660-9-0-1(config)# ip access-list extended eacl-out2in
C3660-9-0-1(config-ext-nacl)# deny ip 0.0.0.0 1.255.255.255 any
C3660-9-0-1(config-ext-nacl)# deny ip 2.0.0.0 0.255.255.255 any
C3660-9-0-1(config-ext-nacl)# deny ip 5.0.0.0 0.255.255.255 any
此处省略部分显示...
C3660-9-0-1(config-ext-nacl)# deny ip 224.0.0.0 31.255.255.255 any
C3660-9-0-1(config-ext-nacl)# deny ip 200.100.14.0 0.0.0.127 any
C3660-9-0-1(config-ext-nacl)# evaluate rf-tcp
C3660-9-0-1(config-ext-nacl)# evaluate rf-udp
```

```
C3660-9-0-1(config-ext-nacl)# evaluate  rf-icmp
C3660-9-0-1(config-ext-nacl)# permit  tcp  any  200.100.14.112  0.0.0.7  eq  22
C3660-9-0-1(config-ext-nacl)# permit  tcp  any  host  PCb 的 IP 地址  eq  80
C3660-9-0-1(config-ext-nacl)# permit  tcp  any  host  PCb 的 IP 地址  eq  21
C3660-9-0-1(config-ext-nacl)# permit  tcp  any  host  PCb 的 IP 地址  eq  20
C3660-9-0-1(config-ext-nacl)# permit  icmp  any  host  PCb 的 IP 地址
C3660-9-0-1(config-ext-nacl)# deny  tcp  any  any
C3660-9-0-1(config-ext-nacl)# deny  udp  any  any
C3660-9-0-1(config-ext-nacl)# deny  icmp  any  any
C3660-9-0-1(config-ext-nacl)# permit  ip  any  any
C3660-9-0-1(config-ext-nacl)# exit
C3660-9-0-1(config)# interface  fa0/1
C3660-9-0-1(config-if)# ip  access-group  eacl-out2in  in
```

配置完成后，在模拟外网主机 PCc 上运行浏览器程序，测试能否访问内网的 HTTP、FTP 服务器 PCb。同时在 PCb、PCc 使用 Wireshark 软件，观察 FTP 客户端能否与 FTP 服务器正常建立下载连接。

测试能否在模拟内网主机 PCa 上运行浏览器程序，测试能否访问外网的 HTTP、FTP 服务器 PCc。同时在 PCa、PCc 使用 Wireshark 软件，观察 FTP 客户端能否与 FTP 服务器正常建立下载连接。

使用 show ip access-lists 命令检查 ACL 匹配情况，检查是否有动态反射 ACL 条目产生。

(2) 配置 CBAC，禁止外网对内网的主动 TCP、UDP、ICMP 连接。根据 2.6 节方案 1，在路由器接口的恰当方向上配置 CBAC 及 ACL，禁止外网对内网的主动 TCP、UDP、ICMP 连接。配置步骤如下。

```
C3660-1-0-1(config)# ip  inspect  name  cbac  tcp
C3660-1-0-1(config)# ip  inspect  name  cbac  udp
C3660-1-0-1(config)# ip  inspect  name  cbac  icmp
C3660-1-0-1(config)# ip  inspect  tcp  max-incomplete  host  100
C3660-1-0-1(config)# ip  inspect  tcp  synwait-time  5
C3660-1-0-1(config)# ip  inspect  udp  idle-time  5
C3660-1-0-1(config)# interface  fa0/1
C3660-1-0-1(config-if)# ip  inspect  cbac  out
C3660-1-0-1(config-if)# exit
C3660-9-0-1(config)# ip  access-list  extended  eacl-out2in
C3660-9-0-1(config-ext-nacl)# deny  ip  0.0.0.0  1.255.255.255  any
C3660-9-0-1(config-ext-nacl)# deny  ip  2.0.0.0  0.255.255.255  any
C3660-9-0-1(config-ext-nacl)# deny  ip  5.0.0.0  0.255.255.255  any
此处省略部分显示...
C3660-9-0-1(config-ext-nacl)# deny  ip  224.0.0.0  31.255.255.255  any
C3660-9-0-1(config-ext-nacl)# deny  ip  200.100.14.0  0.0.0.127  any
C3660-9-0-1(config-ext-nacl)# permit  tcp  any  200.100.14.112  0.0.0.7  eq  22
C3660-9-0-1(config-ext-nacl)# permit  tcp  any  host  PCb 的 IP 地址  eq  80
C3660-9-0-1(config-ext-nacl)# permit  tcp  any  host  PCb 的 IP 地址  eq  21
C3660-9-0-1(config-ext-nacl)# permit  tcp  any  host  PCb 的 IP 地址  eq  20
C3660-9-0-1(config-ext-nacl)# permit  icmp  any  host  PCb 的 IP 地址
C3660-9-0-1(config-ext-nacl)# deny  tcp  any  any
```

```
C3660-9-0-1(config-ext-nacl)# deny   udp   any   any
C3660-9-0-1(config-ext-nacl)# deny   icmp   any   any
C3660-9-0-1(config-ext-nacl)# permit   ip   any   any
C3660-9-0-1(config-ext-nacl)# exit
C3660-9-0-1(config)# interface   fa0/1
C3660-9-0-1(config-if)# ip   access-group   eacl-out2in   in
```

配置完成后，在模拟外网主机 PCc 上运行浏览器程序，测试能否访问内网的 HTTP、FTP 服务器 PCb。同时在 PCb、PCc 使用 Wireshark 软件，观察 FTP 客户端能否与 FTP 服务器正常建立下载连接。

测试能否在模拟内网主机 PCa 上运行浏览器程序，测试能否访问外网的 HTTP、FTP 服务器 PCc。同时在 PCa、PCc 使用 Wireshark 软件，观察 FTP 客户端能否与 FTP 服务器正常建立下载连接。

使用 show ip access-lists 命令检查 ACL 匹配情况。

(3) Smurf、TFN 网络攻击防护。在 PCc 上运行网络攻击软件 Smurf 对模拟分支机构网络内主机 PCa 发动 ICMP DoS 攻击，并在路由器上使用 show ip access-lists 命令检查 ACL 匹配情况，查看是否有大量 ICMP 流量被丢弃。在 PCc 上使用 Wireshark 软件观察 Smurf 发出的攻击流量特点。

在 PCc 上运行网络攻击软件 TFN 对模拟分支机构网络内主机 PCa 发动 TCP SYN 攻击，并在路由器上使用 show ip access-lists 命令检查 ACL 匹配情况，查看是否有大量 TCP 流量被丢弃；使用 show ip inspect 命令检查 TCP 半连接数量。在 PCc 上使用 Wireshark 软件观察 TFN 发出的攻击流量特点。

7. 实训报告

1. 网络连接情况

接口	IP/网络前缀	VLAN 编号	网关地址
路由器接口 Fa0/1	________	/	/
路由器子接口	________	99	/
路由器子接口	________	10	________
路由器子接口	________	20	________
路由器管理地址	________	________	________
交换机管理地址	________	________	________
PCa	________	________	________
PCb	________	________	________
PCc	________	________	________

2. 根据反射 ACL 实训结果回答问题

如果将反射 ACL eacl-in2out 中的 3 条反射 ACL 条目定义去掉，改为 1 条 permit ip any any rf-ip 是否可以成功，与使用 3 条反射 ACL 条目的区别是什么？

续表

3. 根据反射 ACL 实训结果回答问题 （1）在配置了反射 ACL 条目后，内网主机 PCa 能否从 PCc 下载文件？为什么？ （2）在配置了反射 ACL 条目后，主机 PCc 能否从 PCb 下载文件？为什么？
4. 根据 CBAC 实训结果回答问题 配置 CBAC 并从 PCa 访问 PCc 后，CBAC 产生的动态 ACL 条目被放置在哪个 ACL 中的什么位置？
5. 根据 CBAC 实训防护 Smurf 攻击结果回答问题 （1）记录使用 show access-lists 检查所配置的 ACL 防护 Smurf 攻击的输出结果。 （2）记录使用 show access-lists 检查所配置的 ACL 防护 TFN 攻击的输出结果。

第 3 章

局域网安全

本章任务： 根据工程任务安全需求分析，解决局域网中安全配置问题。

必备知识：（1）AAA 技术。
（2）端口安全技术。
（3）IEEE 802.1.x。
（4）交换机访问控制。
（5）DHCP 监听。
（6）IP 源防护。
（7）动态 ARP 检测。
（8）私有 VLAN。
（9）VLAN 跳跃攻击。

学习目标： 完成模拟公司总部局域网的网络安全配置，防御局域网内常见安全威胁。

3.1 模拟网络局域网安全任务分析

模拟公司总部局域网拓扑示意图如图 3-1 所示，用户数据流量由分布在各楼层的二层交换机接入网络，又经分布在各楼宇的三层交换机汇聚，最终进入位于网络中心的核心交换机高速转发。在这样的交换网络中，可能会存在以下安全问题而影响网络的正常运行：

（1）模拟公司总部局域网中使用了大量 Cisco 产品，容易遭受各类针对 Cisco 网络产品的网络攻击威胁，例如 CDP 攻击、VTP 攻击等。

（2）网管员拟用 Telnet 对模拟公司总部局域网网络设备进行远程配置管理。但 Telnet 协议使用明文传输方式进行通信，易被恶意用户窃听而暴露网络设备管理配置信息，即遭遇 Telnet 攻击。

（3）由于从 Internet 上可以非常容易获得各类局域网攻击工具，因此模拟公司总部网络有被恶意用户进行诸如 MAC 地址泛洪、MAC 地址欺骗、ARP 欺骗、DHCP 欺骗攻击的安全风险。而一些网络病毒，例如 ARP 病毒则更有可能让公司计算机在毫不知情下发动 ARP 攻击。

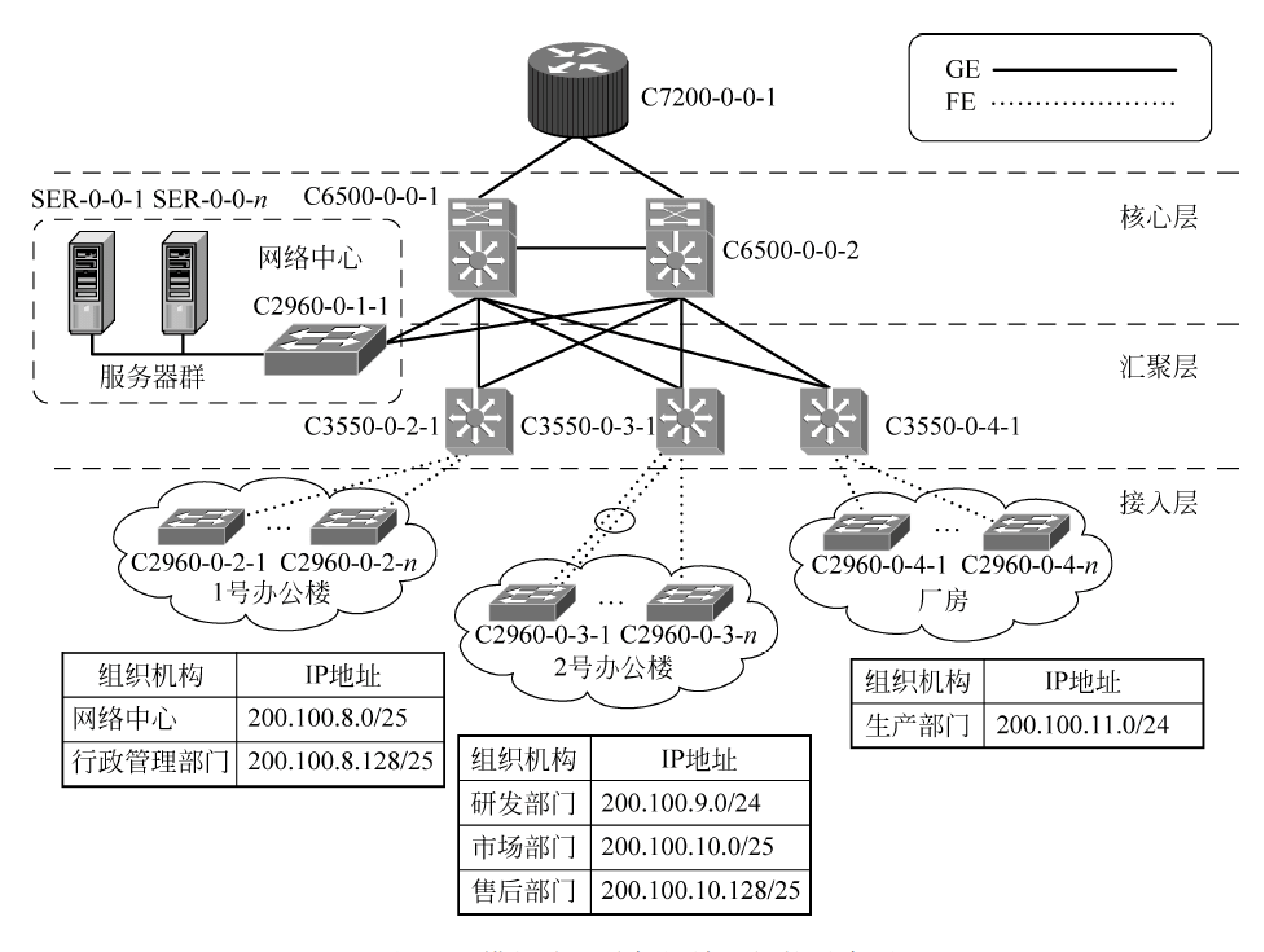


图 3-1 模拟公司总部局域网拓扑示意图

(4) 按照公司网络安全管理制度,模拟公司的总部局域网中不允许用户随意接入网络设备,但由于办公网络的开放性,很难保证用户不会为了拓展网络范围或其他目的而私自向网络中接入交换机、集线器,从而使总部局域网面临 VLAN 跳跃攻击、同 VLAN 内主机间攻击、非授权设备接管 STP 根、VLAN 环路、非授权集线器或交换机接入网络等各种潜在网络安全风险;同时也难以保证有恶意用户未经授权接入办公网络。

要解决以上网络安全问题,可在模拟公司总部局域网中实施以下局域网安全配置方案,以保障网络安全。表 3-1 为该配置方案安全任务列表。

表 3-1 模拟公司总部局域网安全配置任务列表

常见攻击类别	常见攻击方法	相应安全配置任务
对网络设备的攻击	CDP 攻击	禁用不必要端口上的 CDP
	伪造 VLAN 数据库的 VTP 攻击	配置 VTP 域口令
	Telnet 攻击	方法 1:配置 VTY ACL 等对 Telnet 进行访问控制 方法 2:配置 SSH,对远程访问进行加密,并配置 AAA 对 SSH 访问进行安全验证
MAC 层攻击	MAC 地址泛洪	配置端口安全,划分 VLAN
欺骗攻击	DHCP 欺骗	配置 DHCP 监听
	MAC 地址欺骗	配置端口安全
	ARP 欺骗	配置 DAI、DHCP 监听、IP 源防护
	IP 地址欺骗	配置 IP 源防护

续表

常见攻击类别	常见攻击方法	相应安全配置任务
VLAN 攻击	VLAN 跳跃攻击	检查交换机端口模式,务必使非干道端口模式配置为接入模式
	同 VLAN 内主机间攻击	配置 PVLAN,隔离同 VLAN 内主机
STP 攻击	非授权设备接管 STP 根	在接入端口配置"根防护"
	接入非授权集线器或交换机	配置 BPDU 防护,配置端口安全
	VLAN 环路	配置 BPDU 防护,启用 PortFast 特性
非授权主机接入		配置 IEEE 802.1x
内网访问攻击、蠕虫等		配置 PACL、VACL 等

(1) 在网络搭建完成后,禁用总部局域网 Cisco 网络设备不必要端口上的 CDP 协议以防御 CDP 攻击;确保网络中 Cisco 交换机上正确配置了 VTP 域口令,以抵御 VTY 攻击。

(2) 改用 SSH 替代 Telnet 作为远程登录管理网络设备的主要方式,同时配置 AAA 实现远程登录的统一身份验证。对于现有网络中不支持 SSH 功能的 Cisco 网络设备,仍然使用 Telnet,但要使用 VTY、ACL 等访问控制手段加强网络设备的安全保障。

(3) 合理划分 VLAN,并在网络设备上配置端口安全特性以防范 MAC 地址泛洪攻击和 MAC 地址欺骗攻击;配置交换机访问控制,防御网络蠕虫攻击,限制主机间访问;在网络设备上启用并配置 DHCP 监听安全特性,以防范恶意用户假冒 DHCP 服务器、客户端,对网络中的 DHCP 服务进行 DoS 攻击;在网络设备上启用并配置 DAI 安全特性,以防御越来越严重的 ARP 欺骗攻击;在网络设备上配置 IP 源防护,以防御 IP 地址欺骗攻击;在局域网接入交换机上配置 IEEE 802.1x 认证,禁止非授权计算机的接入。

(4) 检查网络中所有交换机的端口模式,务必使非干道端口配置为接入模式;在接入交换机上配置 PVLAN,隔离同 VLAN 内主机;在交换机接入端口上配置"根防护",以防御非授权设备接管"STP 根";在网络设备上配置 BPDU(Bridge Protocol Data Unit,网桥协议数据单元)防护和端口安全特性,防止非授权集线器和交换机接入网络;在网络设备上配置 BPDU 防护,启用相应交换机端口的 PortFast 特性,以防止因用户私接网络设备形成 VLAN 环路。

该安全方案中有关"根防护"、BPDU、PortFast 等生成树安全配置内容,可参见本系列教材中《计算机网络集成技术》一书,本章不再赘述。

3.2 AAA 技术

3.2.1 AAA 及 RADIUS 简介

AAA 是一种网络访问控制体系模型,它支持多种方式进行网络安全访问控制,其中也包括将用户身份信息、授权信息集中保存在 AAA 服务器的数据库中,并集中在 AAA 服务器上进行访问控制的方式。因此,网络中常利用 AAA 来实施集中验证、授权访问控制。

AAA 是"身份验证、授权和记账"(Authentication、Authorization、Accounting)这 3 种网络安全功能的简写。

"验证"是确定用户是谁。是指在用户使用网络系统资源前,对其是否可以获得访问

权限进行检查。

“授权”是确定用户能干什么。是指对已通过验证的用户，指定其可以使用的服务和可以拥有的权限。

“记账”是确定用户消耗了多少网络资源。是指利用网络系统来收集、记录用户使用网络资源情况信息，以便于今后向用户收取资源使用费或进行审计。

当前流行的 AAA 协议是“远程验证拨入用户服务”(Remote Authentication Dial-In User Service，RADIUS)，该协议采用客户端/服务器(Client/Server，C/S)结构，使用 UDP 作为传输协议。RADIUS 客户端可以是任何“网络接入服务器”(Network Access Server，NAS，如路由器、交换机、防火墙等)设备，RADIUS 客户端的任务是将用户的信息发送到指定的服务器，然后根据服务器的不同响应进行相应处理，如接入/挂断用户等；RADIUS 服务器通常运行于一台工作站上，其任务是接收 RADIUS 客户端发来的请求，验证用户身份，并返回 RADIUS 客户端向用户提供服务时所需的配置信息。RADIUS 服务器的数据库中存放着用户验证和网络服务访问的相关信息。

图 3-2 为交换机使用 RADIUS 进行集中验证授权的示意图。用户访问交换机前，需要通过交换机上的网络接入服务器(RADIUS 客户端)向 RADIUS 服务器确认用户的身份，一旦身份验证通过，用户就可以根据授权访问该交换机。

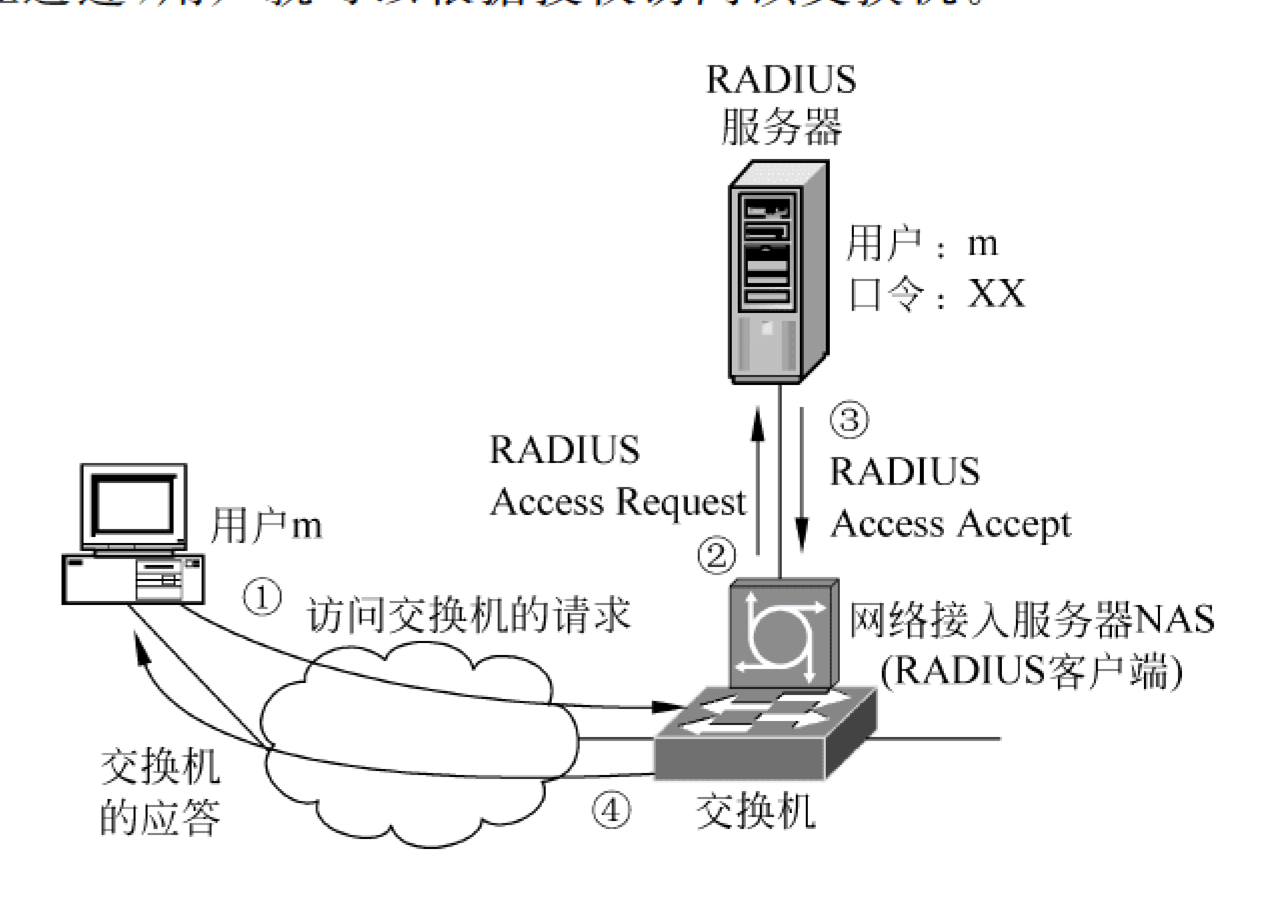


图 3-2　使用 RADIUS 进行集中验证授权示例

RADIUS 客户端与服务器间通信过程如图 3-3 所示。RADIUS 服务器使用 1645、1646 两个 UDP 端口与 RADIUS 客户端进行通信，其中 1645 用于身份验证与授权，1646 用于记账(注意，新的 RADIUS 服务器也可使用 1812、1813 两个 UDP 端口)。

用户登录触发 NAS 发送一个 Access-Request 类型的 RADIUS 协议报文分组到 RADIUS 服务器。该分组中包括用户名、使用共享密钥加密的用户密码、RADIUS 客户端与服务器的共享密钥、NAS 的 IP 地址及端口、用户希望的会话类型(用户 Telnet 到网络设备时为 Service-Type＝Shell，用户 PPP 连接到网络设备时为 Service-Type＝Framed-User 和 Framed-Type＝PPP)等信息。

RADIUS 服务器收到 Access-Request 分组后，首先检查其中的共享密钥，确保该客户端的共享密钥与服务器端的一致。如果共享密钥错误，服务器将丢弃该分组，也不发送

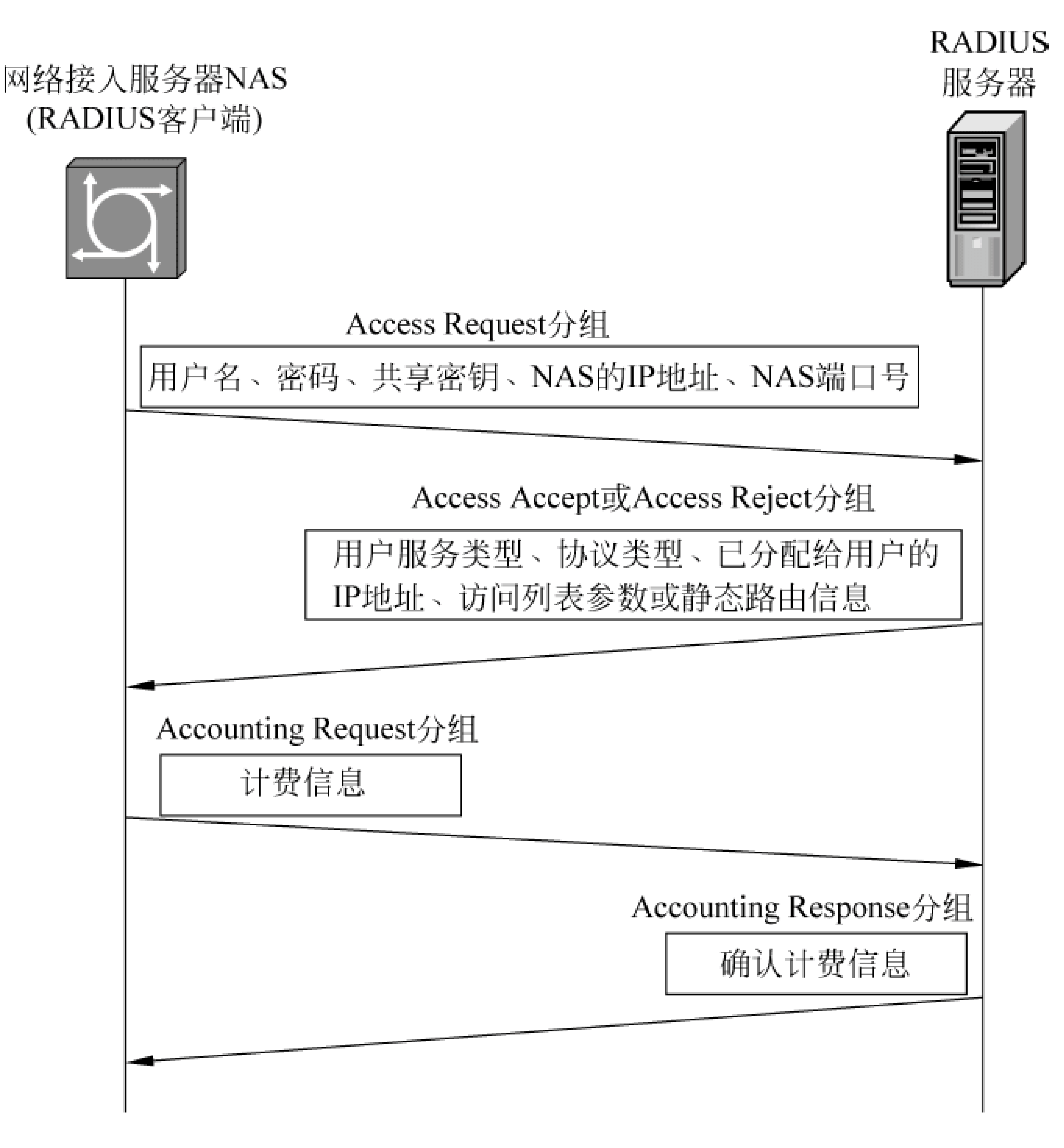


图 3-3 RADIUS 客户端与 RADIUS 服务器通信过程

任何响应信息；如果密钥正确，服务器则将该分组中的信息与数据库中的信息进行对比。

如果数据库中存在该分组信息中的用户名，且密码有效，则服务器向客户端返回 Access-Accept 响应。Access-Accept 中包含一个属性/值对的列表，定义了用户希望发起的会话所要用到的一些参数。例如服务类型(Shell 或 Framed)、协议类型、已分配给用户的 IP 地址、访问列表参数或 NAS 路由选择表中的静态路由信息。

如果数据库中检索不到用户名或密码错误，则 RADIUS 服务器向客户端返回 Access-Reject 响应。

注意，RADIUS 授权失败，服务器也会发送 Access-Reject 响应。

3.2.2 AAA 配置方法

配置基于 RADIUS 协议的网络设备 AAA 访问控制操作主要包括以下步骤。

(1) 在网络中安装设置一台或多台 RADIUS 服务器。

(2) 在网络设备上配置 RADIUS 客户端。

1. RADIUS 服务器安装与配置

由于 Cisco 公司开发的 RADIUS 服务器软件 Cisco ACS 需要付费购买，在实际应用中很多企业为降低成本往往选用免费开源 RADIUS 服务器软件。FreeRADIUS 是一款知名的基于 Linux 平台开源 RADIUS 服务器软件，可以提供身份验证、授权、记账等 AAA 服务功能。FreeRADIUS. net 是用 FreeRADIUS 源码在 Windows 平台上编译形成的一个

FreeRADIUS Windows 版本，本书以 FreeRADIUS.net 软件为例介绍 RADIUS 的配置。

安装配置 FreeRADIUS.net 服务器的主要步骤包括：下载安装 FreeRADIUS.net 服务器软件；配置 FreeRADIUS.net 接收 RADIUS 客户端 AAA 请求；配置 FreeRADIUS.net 用户验证、授权、记账配置信息；检查 FreeRADIUS.net 用户验证、授权、记账信息。

（1）下载、安装 FreeRADIUS.net 服务器软件

FreeRADIUS.net 的官方网站地址为 http://www.freeradius.net。将其安装程序压缩包解压缩后直接运行，即可启动安装 FreeRADIUS.net。

FreeRADIUS.net 安装过程如图 3-4～图 3-7 所示，选项默认即可。



图 3-4　FreeRADIUS.net 安装欢迎界面

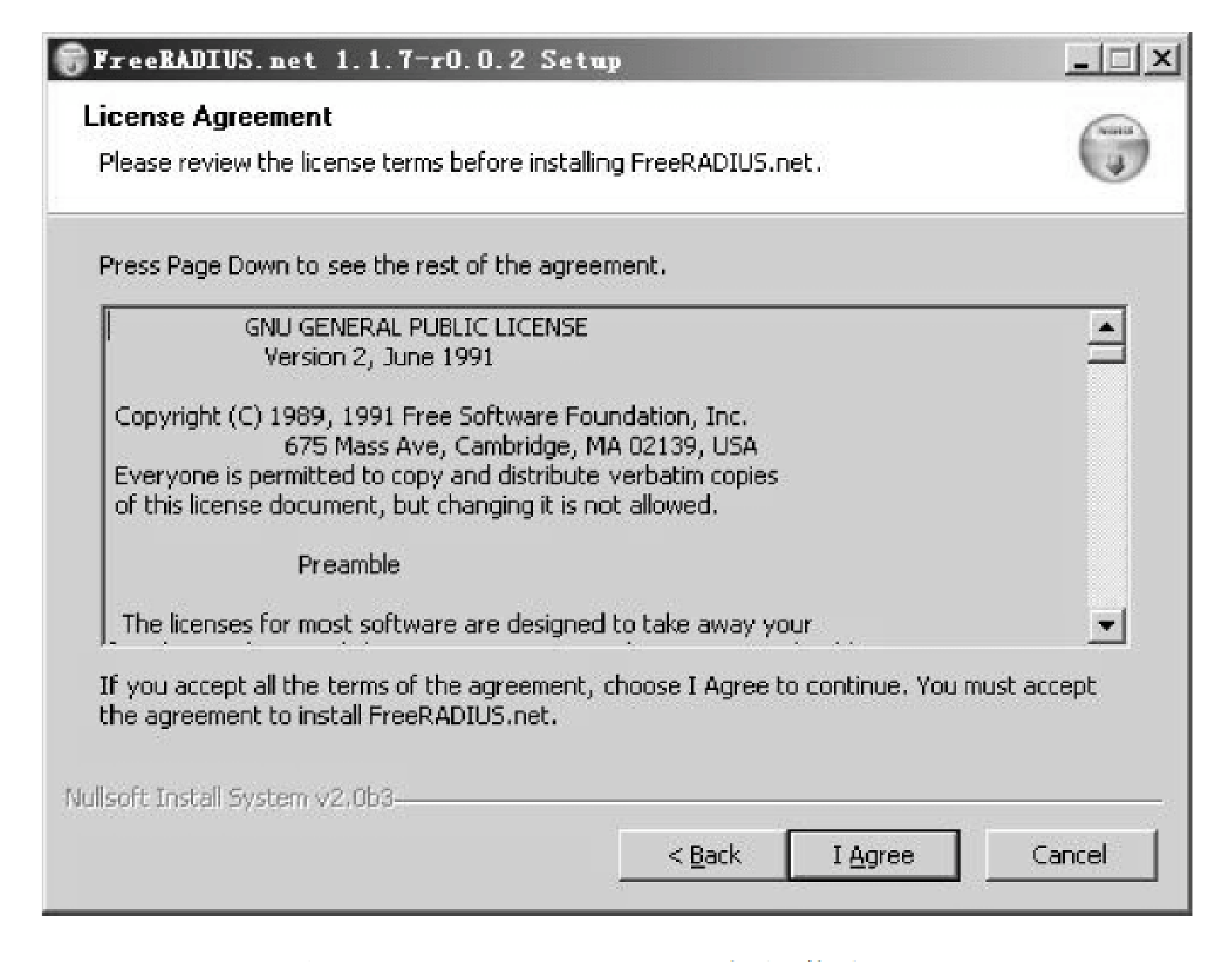


图 3-5　FreeRADIUS.net 版权信息界面

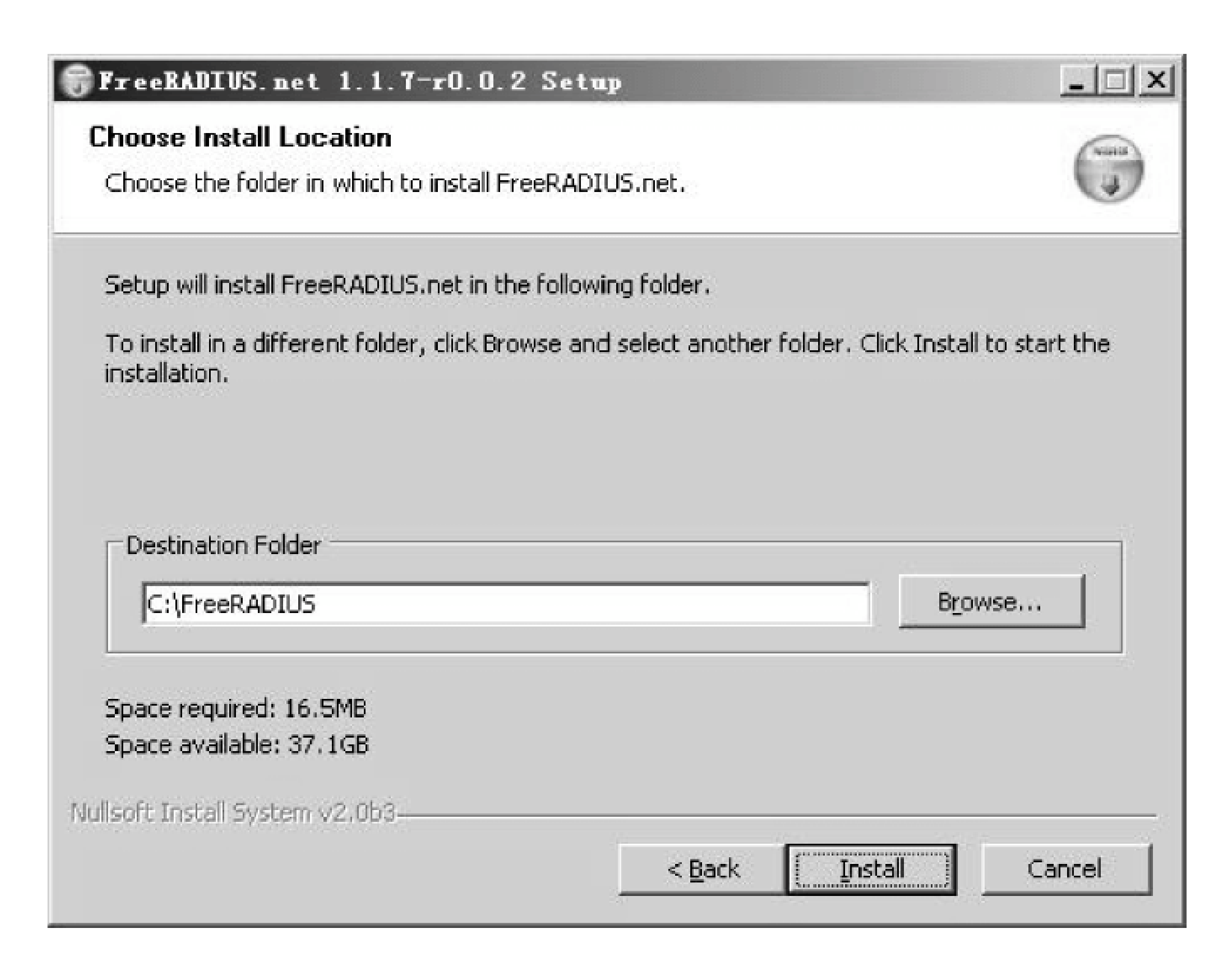


图 3-6　配置 FreeRADIUS. net 安装路径

在安装 FreeRADIUS. net 后进入安装目录，双击运行 FreeRADIUS. exe，此时在系统托盘处会出现 FreeRADIUS 服务的控制程序图标。

右击图标，在弹出如图 3-8 所示的快捷菜单中选择 Start FreeRADIUS. net in DEBUG Mode 命令以调试方式启动 FreeRADIUS 服务。



图 3-7　FreeRADIUS. net 安装完成界面

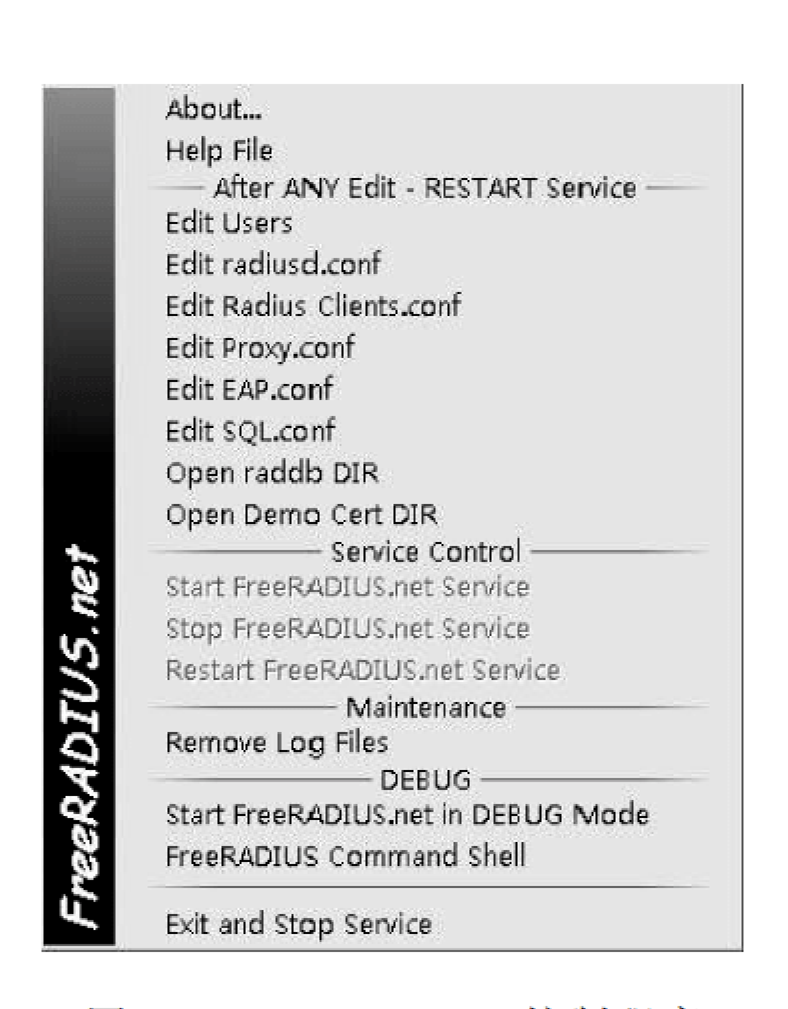


图 3-8　FreeRADIUS 控制程序的快捷菜单

如果出现图 3-9 所示的窗口，其中显示了如下信息。

```
Listening on authentication * :1812
Listening on accounting * :1813
```

Ready to process requests.

这意味着 FreeRADIUS. net 服务器已经成功安装，并分别使用 1812、1813 作为身份验证/授权和记账服务通信端口开始监听客户端请求。

```
C:\Windows\system32\cmd.exe
 radutmp: perm = 511
 radutmp: callerid = yes
Module: Instantiated radutmp (radutmp)
 detail: detailfile = "../var/log/radius/radacct/%{Client-IP-Address}/pre-proxy-
detail-%Y%m%d.log"
 detail: detailperm = 511
 detail: dirperm = 493
 detail: locking = no
Module: Instantiated detail (pre_proxy_log)
 detail: detailfile = "../var/log/radius/radacct/%{Client-IP-Address}/post-proxy
-detail-%Y%m%d.log"
 detail: detailperm = 511
 detail: dirperm = 493
 detail: locking = no
Module: Instantiated detail (post_proxy_log)
 detail: detailfile = "../var/log/radius/radacct/%{Client-IP-Address}/reply-deta
il-%Y%m%d.log"
 detail: detailperm = 511
 detail: dirperm = 493
 detail: locking = no
Module: Instantiated detail (reply_log)
Listening on authentication *:1812
Listening on accounting *:1813
Ready to process requests.
_
```

图 3-9　FreeRADIUS. net 调试模式运行的窗口

注意： 可以根据实际需求配置 FreeRADIUS. net 在哪些端口上监听请求，但若没有配置，则 FreeRADIUS. net 会按照系统 Services 文件中的 RADIUS 端口相关定义工作。Windows 系统 Services 文件一般保存在 C:\Windows\system32\drivers\etc 目录下面。

此时在 CMD 窗口输入 netstat -a，应能看到如图 3-10 所示已经打开进行监听的 UDP1812、1813 端口。



图 3-10　使用 netstat 命令检查 RADIUS 监听端口

注意： 此时 FreeRADIUS 服务器按照默认配置工作，只能接收来自本地的 RADIUS 请求。

(2) FreeRADIUS. net 主要配置内容及相关配置文件

初始安装后的 FreeRADIUS. net 服务器程序还需经过配置才能正常工作，注意修改配置后只有重新启动 RADIUS 服务器修改才能生效。FreeRADIUS. net 服务器的主要配置包括：RADIUS 客户端地址；AAA 身份验证信息；AAA 授权信息(可选)；AAA 记账信息(可选)。

FreeRADIUS. net 有关配置文件均保存在其安装目录下的 etc/raddb 子目录中。表 3-2 列出了其主要配置文件及其用途。

表 3-2　FreeRADIUS. net 主要配置文件及用途

配置文件名	用　　途
clients. conf	该文件定义 FreeRADIUS 可以接收请求的 RADIUS 客户端信息
users. conf	该文件是 FreeRADIUS 用于保存用户身份验证、授权信息及如何进行记账的配置文件
radius. conf	该文件是 FreeRADIUS 的主配置文件，在该文件中定义了 FreeRADIUS 服务器程序运行在哪个 IP 地址、端口上，同时还定义了 FreeRADIUS 服务器在哪里保存用户身份验证、授权、记账信息等

(3) 配置 FreeRADIUS 服务器响应的 FreeRADIUS 客户端地址

修改 FreeRADIUS 安装目录下 etc/raadb 子目录下的 clients. conf 文件，在文件末按如下格式为每个 RADIUS 客户端添加一段配置信息。

```
client   RADIUS 客户端 IP 地址/网络前缀长度 {
      secret       =   共享密钥值
      shortname    =   RADIUS 客户端主机名
}
```

例如，如果 RADIUS 客户端的 IP 地址和子网掩码分别为 202. 207. 122. 165，255. 255. 255. 192，共享密钥为 123456，主机名为 2s1，则要让 FreeRADIUS 服务器能处理该客户端的请求，就应为其在 clients. conf 文件末增加以下内容。

```
client   202.207.122.165/26 {                ①
secret =   123456                            ②
shortname =   2s1                            ③
}
```

其中：

① 配置客户端 IP 地址为 202. 207. 122. 165，根据子网掩码计算其网络前缀长度为 26。

② 配置客户端与 RADIUS 服务器间的共享密钥为 123456。

③ 客户端主机名为 2s1。

(4) 配置用户身份验证等信息

修改 FreeRADIUS 安装目录下 etc/raadb 子目录下的 users. conf 文件。在其中最开始位置为每个用户按如下格式增加一行配置信息。

```
用户名      User-Password== "用户密码"
```

除配置用户名、密码外，还可以在该文件中为用户配置验证协议、授权、记账等信息。

(5) 启动/停止 FreeRADIUS. net

右击系统托盘中的 FreeRADIUS. net 图标，在弹出的快捷菜单中选择 Start FreeRADIUS. net Service 命令可以启动 FreeRADIUS. net 服务，选择 Stop FreeRADIUS. net Service 命令可以停止 FreeRADIUS. net 服务。要停止以调试方式运行的 FreeRADIUS. net 服务，可以在其 CMD 窗口中按 Ctrl+C 键，然后输入 Y 即可。

(6) 查看 FreeRADIUS.net 记账信息

按照主配置文件 radiusd.conf 的默认配置，FreeRADIUS.net 在其安装目录下的 var\log\radius\radacct 子目录中保存记账记录。来自不同 NAS 的记账信息会被分别保存在以 NAS IP 地址为目录名的子目录中。默认情况下，每个 NAS 子目录中会有 3 类文件，分别为 auth-detail-日期.log、detail-日期.log、reply-detail-日期.log。其中 auth-detail-日期.log 文件为用户身份验证记录，内容如下。

```
Packet-Type = Access-Request
Fri Jul 31 16:35:16 2009
        NAS-IP-Address = 202.207.122.165
        NAS-Port = 1
        NAS-Port-Type = Virtual
        User-Name = "th"
        Calling-Station-Id = "202.207.122.166"
        User-Password = "123456"
        Client-IP-Address = 202.207.122.165
```

其中：

Packet-Type 行表示 RADIUS 包类型是 Access-Request，即身份验证请求。

NAS-IP-Address 行表示发出身份验证请求的 NAS IP 地址为 202.207.122.165。

NAS-Port-Type 行表示 NAS 上触发验证请求的是对 Virtual 端口的访问，即 vty。

User-Name 行表示请求身份验证的用户名是 th。

Calling-Station-Id 行表示用户从 IP 地址为 202.207.122.166 的主机上访问网络设备。

User-Password="123456"行表示用户输入的用户密码为 123456。

Client-IP-Address 行表示 RADIUS 客户端的 IP 地址为 202.207.122.165。

reply-detail-日期.log 为 RADIUS 服务器响应信息的记账记录，内容为：

```
Packet-Type = Access-Accept
Thu Jul 30 21:55:57 2009
```

Packet-Type 行表示 RADIUS 包类型是 Access-Accept，即接受请求。

detail-日期.log 保存记账记录细节信息，即在 NAS 上配置需要记账的记录，内容如下。

```
Fri Jul 31 16:54:09 2009
        NAS-IP-Address = 202.207.122.165
        NAS-Port = 1
        NAS-Port-Type = Virtual
        User-Name = "th"
        Calling-Station-Id = "202.207.122.166"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = NAS-Prompt-User
        Acct-Session-Id = "00000001"
```

```
Login-Service = Telnet
Login-IP-Host = 202.207.122.164
Acct-Session-Time = 1133
Acct-Delay-Time = 0
Client-IP-Address = 202.207.122.165
Acct-Unique-Session-Id = "212a160b8758bf7b"
Timestamp = 1249030449
```

其中：

Acct-Status-Type = Stop 表示该记账记录是对外连接停止时产生的。

Acct-Authentic = RADIUS 表示产生该记账记录的协议是 RADIUS。

Acct-Session-Id = "00000001"表示该记账会话的 ID 号。

Login-Service = Telnet 表示该记账记录是登录 Telnet 服务事件触发的。

Login-IP-Host = 202.207.122.164 表示该记账记录是登录 IP 地址为 202.207.122.164 的 Telnet 服务器事件触发的。

以上配置显示了用户从 IP 地址为 202.207.122.166 的主机上 Telnet 到 IP 地址为 202.207.122.166 的网络设备，然后又从网络设备 Telnet 到 IP 地址为 202.207.122.164 的服务器等事件的记账记录。其中，detail-日期.log 中的记账记录内容由网络设备的相应记账命令定义。

2. RADIUS 客户端配置

以在 Cisco 网络设备上配置 RADIUS 客户端为例，其主要操作步骤如表 3-3 所示。

表 3-3　RADIUS 客户端配置步骤及相关命令列表

序　号	配 置 项 目		相关命令列表	是否必要
步骤 1	启用网络设备 AAA 特性		aaa new-model	是
步骤 2	配置 RADIUS 服务器的有关信息（如果使用本地数据库，则此步可省）		radius-server host radius-server key	是
步骤 3	定义 AAA 验证方法列表		aaa authentication	是
步骤 4	根据需要，在相应线路或接口上应用 AAA 身份验证	为 vty 连接应用 AAA 身份验证	login authentication	可选
		为 PPP 连接应用 AAA 身份验证	ppp authentication	可选
步骤 5	定义 AAA 授权方法列表		aaa authorization	可选
步骤 6	根据需要在相应线路或接口上应用 AAA 授权	为 vty 连接应用 AAA 授权	authorization	可选
		为 PPP 连接应用 AAA 授权	ppp authorization	可选
步骤 7	定义 AAA 记账方法列表		aaa accounting	可选
步骤 8	根据需要在相应线路或接口上应用 AAA 记账	为 vty 连接应用 AAA 记账	accounting	可选
		为 PPP 连接应用 AAA 记账	ppp accounting	可选

(1) 启用网络设备的 AAA 安全特性

Cisco IOS 默认未启用 AAA 安全特性，因此网络设备要配置使用 AAA，第一步就是要在设备上启用该安全特性。在 Cisco IOS 中，启用 AAA 安全特性的命令为全局配置模

式下输入：

```
aaa new-model
```

(2) 配置 RADIUS 服务器的有关信息

作为 RADIUS 客户端，如果选用到 RADIUS 服务器上验证，则必须知道 RADIUS 服务器在哪里、与 RADIUS 服务器通信使用的共享密钥是什么。

在 Cisco IOS 中，配置 RADIUS 服务器地址的命令为全局配置模式下输入：

radius-server host ｛RADIUS 服务器的 IP 地址或主机名｝［可选参数 …］

表 3-4 显示了该命令中部分常用可选参数的含义。

表 3-4 部分常用 RADIUS 服务器信息参数含义

关 键 字	描 述
acct-port	记账服务通信端口，默认为 1646
auth-port	验证、授权服务通信端口，默认为 1645
key	与服务器间的共享密钥，如配置，则会覆盖 radius-server key 命令配置的共享密钥
retransmit	重试连接服务器的最大次数
timeout	等待 RADIUS 服务器应答的最长时间

如果网络上有多个 RADIUS 服务器，可配置多条 radius-server host 命令。但排在配置文件前面的为主 RADIUS 服务器，后面的为备份 RADIUS 服务器，只有访问主 RADIUS 服务器时，备份 RADIUS 服务器才能起作用。

注意：若需要配置备份 RADIUS 服务，则应配置主 RADIUS 服务器的重试连接次数和超时等待时间，才能保证主 RADIUS 服务器宕机后，客户端能有机会连接到备份 RADIUS 服务器。

在 Cisco IOS 中，配置 RADIUS 客户端、服务器间默认共享密钥的命令为全局配置模式下输入：

radius-server key ｛共享密钥值｝

注意：此处配置的密钥值要与在 RADIUS 服务器上配置的共享密钥保持一致。

例如，若网络中 RADIUS 服务器的 IP 为 202.207.122.169，且该 RADIUS 服务器使用 UDP 1812、1813 作为验证、记账通信端口，而共享密钥为 123456，则相应的配置命令为：

```
radius-server host 202.207.122.169 auth-port 1812 acct-port 1813
radius-server key 123456
```

其中：

配置 RADIUS 服务器 IP 地址为 202.207.122.169，验证端口为 1812，记账端口为 1813。

配置 RADIUS 服务器与客户端的共享密钥为 123456。

(3) 定义 AAA 身份验证方法列表

无论配置 AAA 身份验证、授权还是记账，在 Cisco IOS 中均需先定义方法列表以指

定对用户进行相应访问控制的详细参数。方法列表定义一般包括：对什么事件进行验证、授权和记账；使用默认方法还是自定义方法进行验证、授权和记账；使用什么方式方法进行身份验证、授权、记账；身份验证、授权、记账使用的协议等内容。

在 Cisco IOS 中，定义 AAA 身份验证方法列表的命令为全局配置模式下输入：

aaa　authentication　{ login | ppp | enable | 其他访问方式 }　{ 方法列表名 }　{ 身份验证方法 1 { 身份验证使用的协议 }　[身份验证方法 *n*　{ 身份验证使用的协议 }]　}

aaa authentication 命令可以为远程登录、远程拨号接入等各种访问方式配置身份验证方法，表 3-5 列出了配置身份验证方法列表时常用的一些访问方式关键字及含义。

表 3-5　常用访问方式的身份验证关键字及含义

访 问 方 式	命令关键字	描　　述
登录	login	用于任何基于 ASCII 登录的身份验证，如 Telnet、SSH 和本地 console 等
远程拨号接入	ppp	用于 PPP 协议远程访问接入的身份验证，例如 ISDN、远程拨号等
特权访问	enable	用于特权访问的身份验证

aaa authentication 命令中的“方法列表名”参数字段需配置要定义的方法列表名。该字段使用关键字 default 时，可全局配置一个“已定义默认方法列表”；该字段使用其他自定义的名字，则说明正在配置一个自定义的“命名方法列表”。“命名方法列表”、“已定义默认方法列表”和初始就存在的“默认方法列表”是 Cisco IOS 中 3 类优先级从高到低的方法列表。“命名方法列表”必须使用命令应用到相应线路、接口上，才能生效；如果线路、接口上没有应用命名方法列表，则自动应用“已定义默认方法列表”；如果不存在“已定义默认方法列表”，则自动应用“默认方法列表”。

在 Cisco IOS 中，不同访问方式有多种不同的身份验证方法。其中，login 登录方式以及 PPP 远程拨号接入访问方式的常用身份验证方法如表 3-6 所示；enable 特权访问方式，只能使用 default 验证方法。在一条 aaa authentication 方法列表中，可以定义多个身份验证方法，以作为备份验证方法。

表 3-6　login/ppp 访问常用身份验证方法关键字

身份验证方法	关键字	描　　述	适用的访问方式
特权口令验证	enable	将 enable 口令用于身份验证	login/PPP
远程服务器验证	group	到远程 AAA 服务器上进行验证。若希望进行集中身份验证需要使用该参数	login/PPP
线路口令验证	line	将 line 口令用于身份验证	Login
本地验证	local	使用网络设备本地配置的用户名、密码进行验证	login/PPP
不验证	none	不进行身份验证。建议一般不要使用此关键字	login/PPP
需要就验证	if-needed	只有需要验证时才进行验证	PPP

对于配置使用 group 参数的方法列表，还需配置相应的“身份验证协议”来说明 NAS 网络访问服务器使用什么协议与 AAA 服务器进行通信。Cisco IOS 目前支持的协议如

表 3-7 所示。

表 3-7 身份验证协议类型

身份验证协议	关 键 字	描 述
服务器组	已定义的服务器组名	定义该方法列表可以到哪个服务器组内的 AAA 服务器上进行访问控制处理
RADIUS	RADIUS	到已配置的 RADIUS 服务器进行验证操作
TACACS+	TACACS+	到已配置的 TACACS+服务器进行验证操作，TACACS+为 Cisco 专有 AAA 协议

配置服务器组，可以指定不同 AAA 服务器分别完成不同访问控制。例如可以配置两个组分别验证 Telnet 到网络设备和使用远程拨号接入方式访问网络设备。在 Cisco IOS 中，定义服务器组的有关命令为全局配置模式下输入：

aaa group server ｛服务器组名｝

在进入相应服务器组配置模式后，使用以下子命令定义该组中有哪些成员 AAA 服务器。

server ｛服务器主机名或 IP 地址｝

例如，创建名为 tel-ras 的命名方法列表，以对用户 Telnet 远程登录网络设备进行基于 RADIUS 的身份验证，则相应配置命令为在全局配置模式下输入：

```
r0(config)#aaa authentication login tel-ras group radius        ①
r0(config)#radius-server host 202.207.122.169                   ②
r0(config)#radius-server key 123456                             ③
```

其中：

① 创建用于远程登录网络设备的 tel-ras 命名方法列表，该身份验证将到后面配置的 RADIUS 服务器上进行验证。

② 配置 RADIUS 服务器 IP 地址。

③ 配置 RADIUS 客户端与服务器通信的共享密钥。

例如，分别创建名为 tel-sg、ppp-sg 的服务器组，以及名为 tel-ras、ppp-ras 的身份验证命名方法列表，以实现到不同 RADIUS 服务器上对用户 Telnet、PPP 连接进行身份验证。其中，验证 Telnet 连接的 RADIUS 服务器 IP 地址为 202.207.122.169，验证 PPP 连接的 RADIUS 服务器 IP 地址为 202.207.122.168。具体相关配置命令为：

```
r0(config)#aaa group server radius tel-sg                       ①
r0(config-sg-radius)#server 202.207.122.169                     ②
r0(config-sg-radius)#exit
r0(config)#aaa group server radius ppp-sg                       ③
r0(config-sg-radius)#server 202.207.122.168                     ④
exit
r0(config)#aaa authentication login tel-ras group tel-sg        ⑤
r0(config)#aaa authentication ppp ppp-ras group tel-sg          ⑥
```

```
r0(config)#radius-server  host  202.207.122.169     ⑦
r0(config)#radius-server  host  202.207.122.168     ⑧
r0(config)#radius-server  key  123456               ⑨
```

以上各行操作含义如下。

① 创建 tel-sg 服务器组，该组服务器使用 RADIUS 协议。

② 进入 tel-sg 服务器组配置模式，配置服务器 202.207.122.169 为该组内服务器。

③ 创建 ppp-sg 服务器组，该组服务器使用 RADIUS 协议。

④ 进入 ppp-sg 服务器组配置模式，配置服务器 202.207.122.168 为该组内服务器。

⑤ 创建远程登录 login 验证方法列表 tel-ras，它使用服务器组 tel-sg 验证。

⑥ 创建远程拨号接入 PPP 登录验证方法列表 ppp-ras，它使用服务器组 ppp-sg 验证。

⑦ 配置一个 RADIUS 服务器 IP 为 202.207.122.169。

⑧ 配置一个 RADIUS 服务器 IP 为 202.207.122.168。

⑨ 配置 RADIUS 客户端与 RADIUS 服务器的共享密钥为 123456。

(4) 应用 AAA 身份验证方法

命名方法列表必须在相应线路或接口上应用才能生效。在 Cisco IOS 中，不同线路、接口上应用方法列表的命令也有所不同。

在线路上，应用登录身份验证的命令为在线路配置模式下输入：

login authentication {方法列表名}

其中“方法列表名”为使用 aaa authentication 命令定义的命名方法列表名或 default。

为 PPP 接入应用身份验证方法列表的命令为在 PPP 配置模式下输入：

ppp authentication {验证协议} {方法列表名}

例如，若要分别对用户远程登录和远程拨号接入网络设备进行基于 RADIUS 的身份验证，并已定义好对应名为 tel-ras 和 ppp-ras 的命名方法列表，则可以在全局配置模式输入以下命令。

```
Router(config)#line vty 0 4
Router(config-line)#login authentication tel-ras
Router(config-line)#exit
Router(config)#Interface xx
Router(config-if)#ppp authentication chap ppp-ras
```

其中，远程登录使用方法列表 tel-ras 进行登录身份验证；PPP 接入时使用 chap 进行验证，而 chap 验证的方法由 ppp-ras 定义。

(5) 定义 AAA 授权方法列表

定义 AAA 授权方法列表的目的是告诉 RADIUS 客户端授予用户哪些权限。RADIUS 协议将身份验证与授权绑定在一起进行，不如 TACACS+ 协议灵活，所支持的权限类别有限，例如不支持对 Cisco 命令级别等权限的授权。

在 Cisco IOS 中，定义 AAA 授权方法列表的命令为在全局配置模式下输入：

aaa authorization ｛权限类别｝｛方法列表名｝｛授权方法 ｛授权协议｝｝

在 aaa authorization 命令中，“权限类别”参数用于说明对哪类权限进行授权控制，表 3-8 显示了 aaa authorization 命令中可以用于 RADIUS 授权的部分常用权限类别。

表 3-8 Cisco RADIUS 常用权限类别

权限类别	关键字(参数值)	描述
授权代理	auth-proxy	配置授权代理后，用户访问网络前，先需通过 Web 浏览器向 RADIUS 服务器证明其身份，当用户成功通过身份验证后，RADIUS 将 ACL 条目和配置文件信息传递给网络设备，授予用户继续访问网络的权限
用户配置模式	exec	用户通过验证后会进入 exec 即用户配置模式。此项配置用于对远程拨号接入用户进行授权，使用 Telnet、SSH 远程登录的用户，在成功通过身份验证后已经进入 exec 模式，不需要再对此项访问进行授权
网络连接	network	对用户进行网络连接(PPP、SLIP、ARAP)进行相应授权
反向 Telnet	reverse-access	对用户在成功通过身份验证登录网络设备后，Telnet 到其他设备的访问进行授权

在 aaa authorization 命令中，“方法列表”和“授权协议”参数的配置方法参见身份验证中有关说明。

在 aaa authorization 命令中，“授权方法”参数用于说明网络设备到哪里对用户进行授权处理，授权方法根据不同的“权限类别”有所区别。部分常用授权方法如表 3-9 所示。

表 3-9 常用授权方法

授权方法	关键字	描述
远程服务器授权	group	到 group 后所定义的服务器上进行相应授权控制的处理
通过验证就获得授权	if-authenticated	只要用户通过身份验证就获得相应授权
本地授权	local	在本地数据库中进行授权控制的处理
不授权	none	不进行授权控制的处理

(6) 应用 AAA 授权方法

在 Cisco IOS 中，在线路、接口上应用授权方法列表的命令为在相应线路、接口模式下输入：

authorization ｛权限类别｝｛授权方法列表名｝

有关参数定义参见“定义 AAA 授权方法列表”定义部分相关说明。

(7) 定义 AAA 记账方法列表

在定义 AAA 记账方法列表时，必须明确对哪些事件进行记账，到哪里完成记账处理等信息。在 Cisco IOS 中，定义 AAA 记账方法列表的命令为在全局配置模式下输入：

aaa accounting ｛记账事件｝｛方法列表名｝｛**none** | **start-stop** | **stop-only**｝［**broadcast**］［**group** ｛**radius** | **tacacs+** | 服务器组名｝］

其中,"记账事件"参数用于定义对哪些事件进行记账,用于 RADIUS 的部分常用记账事件如表 3-10 所示。

表 3-10 常用记账事件

记账事件	关键字	描 述
验证代理	auth-proxy	对验证代理事件进行统计
对外连接	connection	对网络设备对外建立的连接,例如 Telnet 进行统计
用户模式会话	exec	对用户模式会话进行统计,例如什么用户登录、退出网络设备
系统事件	system	对系统级事件,例如接口状态变化或路由器重启进行统计(仅支持 default 方法列表)
网络服务	network	对所有网络服务,例如 PPP、NCP 等进行统计

none | start-stop | stop-only 部分用于定义何时建立统计记录。其中 start-stop 表示在事件开始和结束时分别建立统计记录;stop-only 表示只在事件结束时建立一个统计记录;none 表示关闭相应事件的统计记录。

broadcast 参数表示网络设备可以将记账(统计)信息同时发送到多台服务器。

(8) 应用 AAA 记账方法

在 Cisco IOS 中,在线路上应用 AAA 记账方法列表的命令为在线路配置模式下输入命令:

accounting { 记账事件 } { 记账方法列表名 }

在 Cisco IOS 中,在接口上应用 PPP 事件 AAA 记账方法列表的命令为在接口配置模式下输入:

ppp accounting {记账方法列表名 }

以上配置命令中各参数用法可参阅"定义 AAA 记账方法列表"中有关内容。

3. RADIUS 配置排错

RADIUS 配置排错可分服务器端、客户端两部分。FreeRADIUS. net 的排错可以使用调试模式进行,操作方法见前面描述。在 Cisco 网络设备上,进行网络排错的命令如表 3-11 所示。

表 3-11 Cisco 网络设备 RADIUS 排错命令

排错范围	命 令	描 述
身份验证错误	debug aaa authentication	调试 aaa 身份验证配置
	debug radius authentication	调试 RADIUS 身份验证配置
授权错误	debug aaa authorization	调试 aaa 授权配置
记账错误	show accounting	显示记账信息
	debug aaa accounting	调试 aaa 记账配置
	debug radius accounting	调试 RADIUS 记账配置

使用 debug aaa authentication 命令输出示例如下。

```
00:46:49: AAA: parse name=tty1 idb type=-1 tty=-1
00:46:49: AAA: name=tty1 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=1 channel=0
00:46:49: AAA/MEMORY: create_user (0x19C7384) user='NULL' ruser='NULL' ds0=0 port=
'tty1' rem_addr='202.207.122.166' authen_type=ASCII service=LOGIN priv=1 initial_task_id=
'0', vrf= (id=0)                                                              ①
00:46:49: AAA/AUTHEN/START (151585098): port='tty1' list='tel-authen-log' action=
LOGIN service=LOGIN                                                           ②
00:46:49: AAA/AUTHEN/START (151585098): found list tel-authen-log             ③
00:46:49: AAA/AUTHEN/START (151585098): Method=radius (radius)                ④
00:46:49: AAA/AUTHEN (151585098): status = GETUSER
00:46:51: AAA/AUTHEN/CONT (151585098): continue_login (user='(undef)')
00:46:51: AAA/AUTHEN (151585098): status = GETUSER
00:46:51: AAA/AUTHEN (151585098): Method=radius (radius)
00:46:51: AAA/AUTHEN (151585098): status = GETPASS
00:46:54: AAA/AUTHEN/CONT (151585098): continue_login (user='th')             ⑤
00:46:54: AAA/AUTHEN (151585098): status = GETPASS
00:46:54: AAA/AUTHEN (151585098): Method=radius (radius)
00:46:54: AAA/AUTHEN (151585098): status = PASS                               ⑥
```

其中：

① 用户从 IP 地址为 202.207.122.166 的主机上试图远程登录到该网络设备。

② 在网络设备 vty 线路上触发对 login 访问进行验证事件，验证使用 tel-auth-log 身份验证命名方法列表进行。

③ 网络设备找到了 tel-auth-log 身份验证命名方法列表定义。

④ 验证将基于 RADIUS 协议进行。

⑤ 用户输入了 th 用户名。

⑥ 用户输入的用户名和密码通过了验证，状态为 PASS。

使用 debug radius authentication 命令输出示例如下。

```
00:47:00: RADIUS: Pick NAS IP for u=0x1854A74 tableid=0 cfg_addr=0.0.0.0
00:47:00: RADIUS: ustruct sharecount=1
00:47:00: Radius: radius_port_info() success=1 radius_nas_port=1
00:47:00: RADIUS(00000000): Send Access-Request to 202.207.122.166:1812 id 1645/10,
len 74
00:47:00: RADIUS: authenticator CF 7C 36 69 C2 1F F7 CF - A2 75 39 F0 8D B3 C7 BC
00:47:00: RADIUS: NAS-IP-Address      [4]  6   202.207.122.166
00:47:00: RADIUS: NAS-Port            [5]  6   1
00:47:00: RADIUS: NAS-Port-Type       [61] 6   Virtual          [5]
00:47:00: RADIUS: User-Name           [1]  4   "th"
00:47:00: RADIUS: Calling-Station-Id [31] 14  "202.207.122.166"
00:47:00: RADIUS: User-Password       [2]  18  *
00:47:03: RADIUS: Received from id 1645/10 202.207.122.166:1812, Access-Reject, len 20
00:47:03: RADIUS: authenticator CF 57 5B D3 61 E0 0F 4D - B0 46 54 4C 24 43 A2 21
00:47:03: RADIUS: response-authenticator decrypt fail, pak len 20
```

```
00:47:03: RADIUS: packet dump: 030A0014CF575BD361E00F4DB046544C2443A221
00:47:03: RADIUS: expected digest: F93676E09FDB6521376DE9B1C8F4DFCF
00:47:03: RADIUS: response authen: CF575BD361E00F4DB046544C2443A221
00:47:03: RADIUS: request  authen: CF7C3669C21FF7CFA27539F08DB3C7BC
00:47:03: RADIUS: Response (10) failed decrypt
00:47:03: RADIUS: Reply for 10 fails decrypt
```

其中：

Send Access-Request to...表示 NAS 发送 Access-Request 请求到 RADIUS 服务器 202.207.122.166。

Received from id...表示 NAS 收到 RADIUS 服务器返回的 Access-Reject。

RADIUS: Response (10) failed decrypt 表示 RADIUS 服务器返回的响应信息表明共享密钥出现错误。

使用 debug　aaa　accounting 命令输出示例如下。

```
01:02:07: AAA: parse name=tty1 idb type=-1 tty=-1
01:02:07: AAA: name=tty1 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=1 channel=0
01:02:07: AAA/MEMORY: create_user (0x19C7474) user='NULL' ruser='NULL' ds0=0
port='tty1' rem_addr='202.207.122.166' authen_type=ASCII service=LOGIN priv=1 initial_
task_id='0', vrf= (id=0)
01:02:12: AAA/ACCT/EXEC/START User th, port tty1
01:02:12: AAA/ACCT/EXEC: Found list "tel-acc-exec"
01:02:12: AAA/ACCT/EXEC/START User th, Port tty1,
          task_id=2 timezone=UTC service=shell
...
01:02:12: AAA/ACCT: user th, acct type 0 (1966749367): Method=radius (radius)
01:14:25: AAA/ACCT/ACCT_DISC: Found list "tel-acc-exec"
01:14:25: tty1 AAA/DISC: 1/"User Request"
01:14:25: AAA/ACCT/ACCT_DISC: Found list "tel-acc-exec"
01:14:25: tty1 AAA/DISC/EXT: 1020/"User Request"
01:14:25: AAA/ACCT/ACCT_DISC: Found list "tel-acc-exec"
01:14:25: tty1 AAA/DISC: 9/"NAS Error"
01:14:25: AAA/ACCT/ACCT_DISC: Found list "tel-acc-exec"
01:14:25: tty1 AAA/DISC/EXT: 1002/"Unknown"
01:14:25: AAA/ACCT: no attribute "elapsed_time" to replace, adding it
01:14:25: AAA/ACCT/EXEC/STOP: cannot retrieve modem speed
01:14:25: AAA/ACCT/EXEC/STOP User th, Port tty1:
          task_id=2 timezone=UTC service=shell protocol=telnet addr=202.207.122.164
disc-cause=1 disc-cause-ext=1020 connect-progress=44 elapsed_time=733 nas-rx-speed=0 nas-
tx-speed=0
01:14:25: AAA/ACCT: user th, acct type 0 (47767151): Method=radius (radius)
01:14:25: AAA/MEMORY: free_user (0x19C7474) user='th' ruser='NULL' port='tty1'
rem_addr='202.207.122.166' authen_type=ASCII service=LOGIN priv=1
```

其中：

AAA/ACCT/EXEC/START User th, port tty1 表示用户远程登录网络设备触发一个在其 line 线路上配置的 EXEC 类型的 START 记账记录。

AAA/ACCT/EXEC：Found list "tel-acc-exec"表示网络设备在系统中找到了该记账记录对应的 tel-acc-exec 方法列表定义。

AAA/ACCT/EXEC/STOP User th，Port tty1 表示用户从远程访问中退出触发了网络设备 line 线路上配置的 EXEC 类型的 STOP 记账记录。

下面是使用 debug aaa accounting 命令输出的另一个示例。

```
01:08:53: AAA/ACCT/PROG: Updating Connect Progress for ds0 0 to 41
01:08:54: AAA/ACCT/PROG: Updating Connect Progress for ds0 0 to 43
01:08:54: AAA/ACCT/PROG: Updating Connect Progress for ds0 0 to 43
01:08:54: AAA/ACCT/PROG: Updating Connect Progress for ds0 0 to 42
01:08:54: AAA/ACCT/CONN: Found list "tel-acc-con"
01:08:54: AAA/ACCT/CONN/START User th, Port tty1, Location "tty1"
01:08:54: AAA/ACCT/CONN/START User th, Port tty1,
task_id=3 timezone=UTC service=connection protocol=telnet addr=202.207.122.164 cmd=
telnet 202.207.122.164
01:08:54: AAA/ACCT: no attribute "protocol" to replace, adding it
01:08:54: AAA/ACCT: no attribute "addr" to replace, adding it
01:08:54: AAA/ACCT/PROG: Updating Connect Progress for ds0 0 to 47
01:08:54: AAA/ACCT: user th, acct type 1 (2062869378): Method=radius (radius)
01:10:12: AAA/ACCT: no attribute "pre-bytes-in" to replace, adding it
01:10:12: AAA/ACCT: no attribute "pre-bytes-out" to replace, adding it
01:10:12: AAA/ACCT: no attribute "pre-paks-in" to replace, adding it
01:10:12: AAA/ACCT: no attribute "pre-paks-out" to replace, adding it
01:10:12: AAA/ACCT: no attribute "bytes_in" to replace, adding it
01:10:12: AAA/ACCT: no attribute "bytes_out" to replace, adding it
01:10:12: AAA/ACCT: no attribute "paks_in" to replace, adding it
01:10:12: AAA/ACCT: no attribute "paks_out" to replace, adding it
01:10:12: AAA/ACCT: no attribute "elapsed_time" to replace, adding it
01:10:12: AAA/ACCT/CONN/STOP: cannot retrieve modem speed
01:10:12: AAA/ACCT/CONN/STOP User th, Port tty1:
task_id=3 timezone=UTC service=connection protocol=telnet addr=202.207.122.164 cmd=
telnet 202.207.122.164 pre-bytes-in=0 pre-bytes-out=0 pre-paks-in=0 pre-paks-out=0 bytes_in
=291 bytes_out=102 paks_in=49 paks_out=59 connect-progress=47 elapsed_time=78 nas-rx-
speed=0 nas-tx-speed=0
01:10:12: AAA/ACCT/PROG: Updating Connect Progress for ds0 0 to 44
01:10:12: AAA/ACCT: user th, acct type 1 (2687305955): Method=radius (radius)
```

其中：

Updating Connect Progress for ds0 0 to 41 表示用户从网络设备 Telnet 到一个服务器的事件触发了一个在其 line 线路上配置的 connection 类型的记账记录。

AAA/ACCT/CONN：Found list "tel-acc-con"表示网络设备在系统中找到了该记账记录对应的 tel-acc-con 方法列表定义。

AAA/ACCT/CONN/START User th，Port tty1，Location "tty1"表示该事件触发了一个在网络设备 line 线路上配置的 connection 类型的 START 记账记录。

AAA/ACCT/CONN/STOP User th，Port tty1 表示用户退出到服务器的 Telnet 事件触发了在网络设备 line 线路上配置的 connection 类型的 STOP 记账记录。

3.2.3　模拟网络的 AAA 配置

在本书模拟网络中，AAA 被设计用来实现远程登录局域网内交换机、路由器等网络设备时的集中身份验证、对外连接记账等。其中，网络中有两台 RADIUS 服务器作为 AAA 主备服务器，IP 地址分别为 200.100.8.29/26 和 200.100.8.30/26；RADIUS 共享密钥为 Net&Sec@sjzpc；用户登录及登录后的对外网络连接事件都要有记账记录；为防止无法连接 RADIUS 服务器导致的远程登录失败，配置备份身份验证方法为 line，并为此配置本地用户名、口令以及 line 口令。

模拟公司总部局域网中网络设备 AAA 配置模板如下，该配置模板中仍然使用 Telnet 作为远程登录方式，适用于不支持 SSH 的网络设备。

```
username th@sjzpc password let! sjzpc
aaa new-model
aaa group server radius tel-sg
 server 200.100.8.30 auth-port 1812 acct-port 1813
 server 200.100.8.29 auth-port 1812 acct-port 1813
!
aaa authentication login tel-auth-in group tel-sg line
aaa accounting exec tel-acc-exec start-stop group tel-sg
aaa accounting connection tel-acc-conn start-stop group tel-sg
此处省略部分配置…
radius-server host 200.100.8.30 auth-port 1812 acct-port 1813 timeout 3 retransmit 3
radius-server host 200.100.8.29 auth-port 1812 acct-port 1813
!
radius-server key Net&Sec@sjzpc
!
line vty 0 4
  accounting connection tel-acc-conn
  accounting exec tel-acc-exec
login authentication tel-auth-in
  password let! 090812
```

该模拟公司总部局域网中另一个网络设备 AAA 配置模板如下，该配置模板中使用 SSH 作为远程登录方式，适用于支持 SSH 的网络设备。

```
username th@sjzpc password let! sjzpc
aaa new-model
!
aaa group server radius ssh-sg
 server 200.100.8.30 auth-port 1812 acct-port 1813
 server 200.100.8.29 auth-port 1812 acct-port 1813
!
aaa authentication login ssh-auth-in group ssh-sg line
aaa accounting exec ssh-acc-exec start-stop group ssh-sg
aaa accounting connection ssh-acc-conn start-stop group ssh-sg
!
此处省略部分配置…
```

```
radius-server host 200.100.8.30 auth-port 1812 acct-port 1813 timeout 3 retransmit 3
radius-server host 200.100.8.29 auth-port 1812 acct-port 1813
radius-server key Net&Sec@sjzpc
!
line vty 0 4
 accounting connection ssh-acc-conn
 accounting exec ssh-acc-exec
 login authentication ssh-auth-in
 transport input ssh
 password let!090812
```

模拟网络中每台网络设备都需要一个管理地址用于远程管理，有关管理地址分配方法等内容可参考本系列教材中《计算机网络集成技术》一书。

3.3 IEEE 802.1x 技术

3.3.1 IEEE 802.1x 技术简介

IEEE 802.1x 是一个两层安全访问控制标准框架，提供基于端口的网络接入控制，即连接在局域网接入控制设备(例如接入交换机)端口上的用户设备只有通过身份验证，才能通过所连接的端口访问局域网中资源。

IEEE 802.1x 标准框架中，完成端口访问控制有 3 个角色：请求者(IEEE 802.1x 客户端)、授权者(交换机)和认证者(认证服务器)。其中交换机是 IEEE 802.1x 客户端与认证服务器间的中介，它与 IEEE 802.1x 客户端使用封装在以太网帧中的 EAP 消息交换身份验证有关信息，然后将 EAP 消息封装在 RADIUS 报文中，中继给 RADIUS 认证服务器。图 3-11 所示为 IEEE 802.1x 工作过程示意图。

1. 初始化认证

IEEE 802.1x 客户端和交换机任一方都可以初始化认证过程。

IEEE 802.1x 客户端会在用户运行该客户端时，向交换机发出 EAPOL-start 消息来初始化认证过程。交换机收到 EAPOL-start 消息后，会向客户端发出一个 EAP Request/Identity 消息，来请求身份验证所需的用户名；交换机会在启用了端口认证，端口状态由 down 向 up 迁移时，向 IEEE 802.1x 客户端发出一个 EAP Request/Identity 消息，来初始化认证过程。

2. 开始认证

EAP 支持的身份验证的方法有多种，如表 3-12 所示。不同身份验证方法的认证过程有所不同，下面以使用消息摘要 MD5 身份验证方法为例。

无论哪一方初始化认证过程，客户端程序收到交换机发来的 EAP Request/Identity 消息后，会提示用户输入用户名、口令，然后将用户输入的用户名信息封装在 EAP Response/Identity 消息中返回给交换机。

交换机解封装客户端发来的以太网帧，并将其中的 EAP-Response/Identity 消息，封装进 RADIUS Access Request 报文中，送给 RADIUS 服务器进行处理。

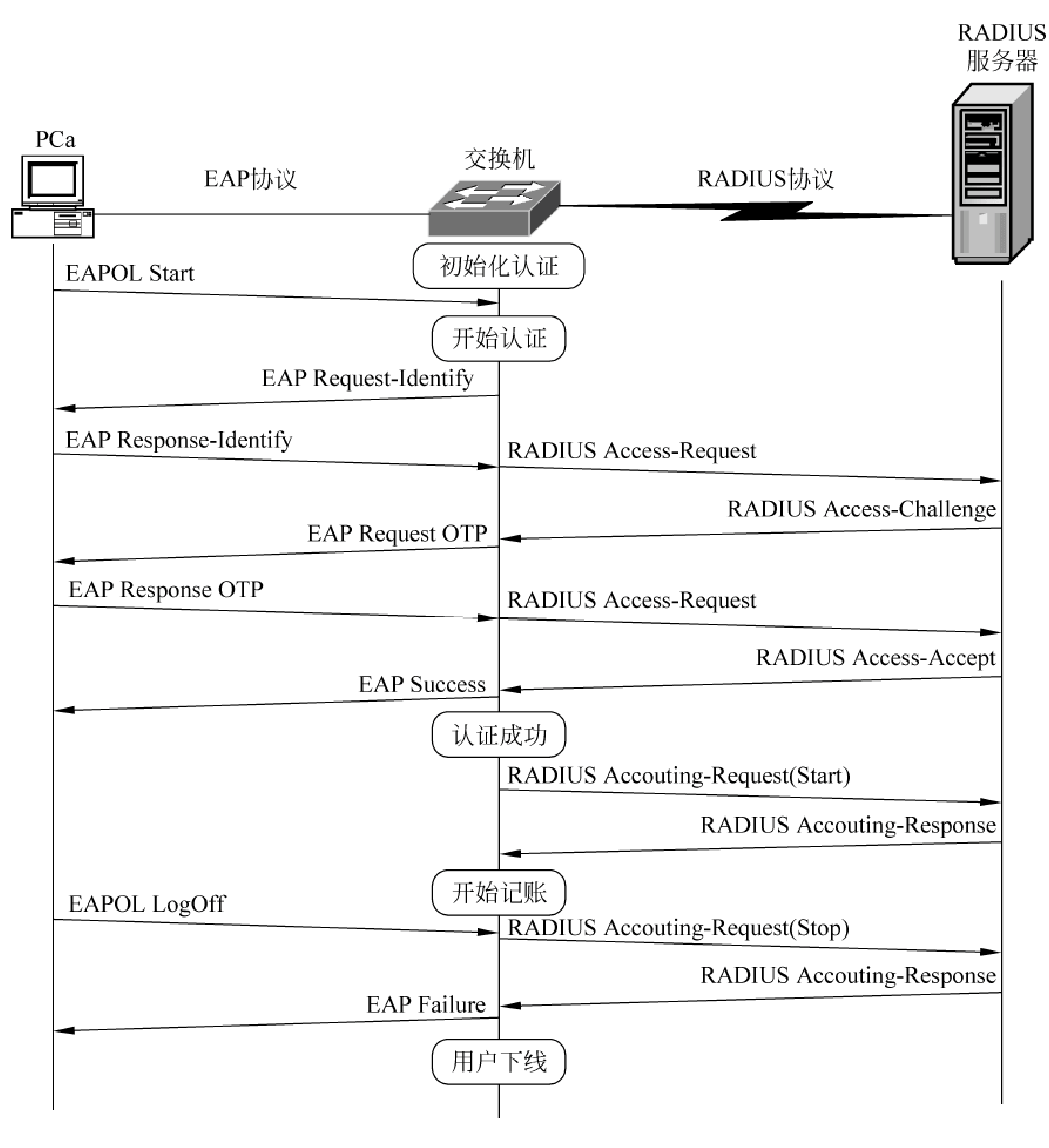


图 3-11　IEEE 802.1x 工作过程示意图

表 3-12　EAP 常用验证方法

身份验证方法	描　　述	Windows XP 802.1x 选项	FreeRADIUS 服务器 EAP 选项
消息摘要 MD5	仅需要服务器证书进行单向认证	MD5-质询	md5
传输层安全 TLS (Transport Layer Security)	用户在客户端与服务器使用 PKI 数字证书进行双向认证	智能卡或其他证书	tls
受保护的扩展认证协议 PEAP(Protected Extensible Authentication Protocol)	PEAP 认证过程中，服务器先向客户端认证，然后在客户端与 RADIUS 服务器间建立一条加密的 TLS 隧道用于传输 EAP 认证信息。该方法支持多种验证方式，包括用户密码和一次性密码，以及“通用令牌卡(Generic Token Card)”	Microsoft：受保护的 EAP	peap

RADIUS 服务器收到交换机转发的用户名信息后，会在数据中找到该用户名对应的口令信息，并用随机生成的一个密钥对口令进行加密处理。然后将密钥通过 RADIUS Access Challenge 报文传送给交换机，再由交换机将其放在 EAP Request OTP 消息中转发给 IEEE 802.1x 客户端。

IEEE 802.1x 客户端收到由交换机中继而来的密钥后，用该密钥加密口令，封装进 EAP Response OTP 消息，并通过交换机封装进 RADIUS Access-Requeset 报文传给 RADIUS 服务器。

RADIUS 服务器将加密后的口令信息和自己经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，将反馈认证通过的消息 EAP Success 消息封装进 RADIUS Access-Accept 报文中发送给交换机。

交换机收到 RADIUS Access-Accept 报文后将端口状态改为授权状态，允许用户通过该端口访问网络。

在此过程中，如果交换机有相应记账配置，则会向 RADIUS 服务器发送相应记账请求，RADIUS 服务器返回响应并进行记账。

3. 断开连接

当用户主动断开连接时，IEEE 802.1x 客户端会发送 EAPOL LogOff 报文给交换机，主动终止已认证状态，交换机将端口状态从授权状态改变成未授权状态。

3.3.2 IEEE 802.1x 配置方法

IEEE 802.1x 的实施需要以下组件。

(1) 用户主机上安装配置 IEEE 802.1x 客户端。

(2) 配置交换机的 IEEE 802.1x 安全特性。

(3) 安装配置 RADIUS 服务器。

有关 RADIUS 服务器安装配置内容参见 3.2.2 小节。

1. 安装配置 IEEE 802.1x 客户端

IEEE 802.1x 客户端软件有独立软件和系统组件两种形式，独立软件需要另外安装。此处以系统组件形式为例。

(1) 开启 Windows 网络连接的 IEEE 802.1x 认证服务

Windows XP SP2 系统已经带有 IEEE 802.1x 客户端软件，但默认没有运行该软件。要运行该软件，可单击“打开”按钮，选择“控制面板”|“管理工具”|“服务”命令，打开“服务”窗口，右击 Wired AutoConfig 选项，在弹出的快捷菜单中选择“启动”命令，启动该服务。启用 Windows 系统上的 IEEE 802.1x 认证服务如图 3-12 所示。

(2) 配置 Windows 网络连接的 IEEE 802.1x 认证

IEEE 802.1x 客户端配置的核心操作是定义 IEEE 802.1x 认证使用的认证方法。在 Windows 系统中定义 IEEE 802.1x 认证方法的操作如下。

启动 Wired AutoConfig 服务后，打开网络连接属性对话框，如图 3-13 所示，可以看到“身份验证”选项卡。选择该选项卡，配置 IEEE 802.1x 认证有关信息。

选中“启用 IEEE 802.1x 身份验证”复选框，在该网络连接上启用 IEEE 802.1x 身份验证。

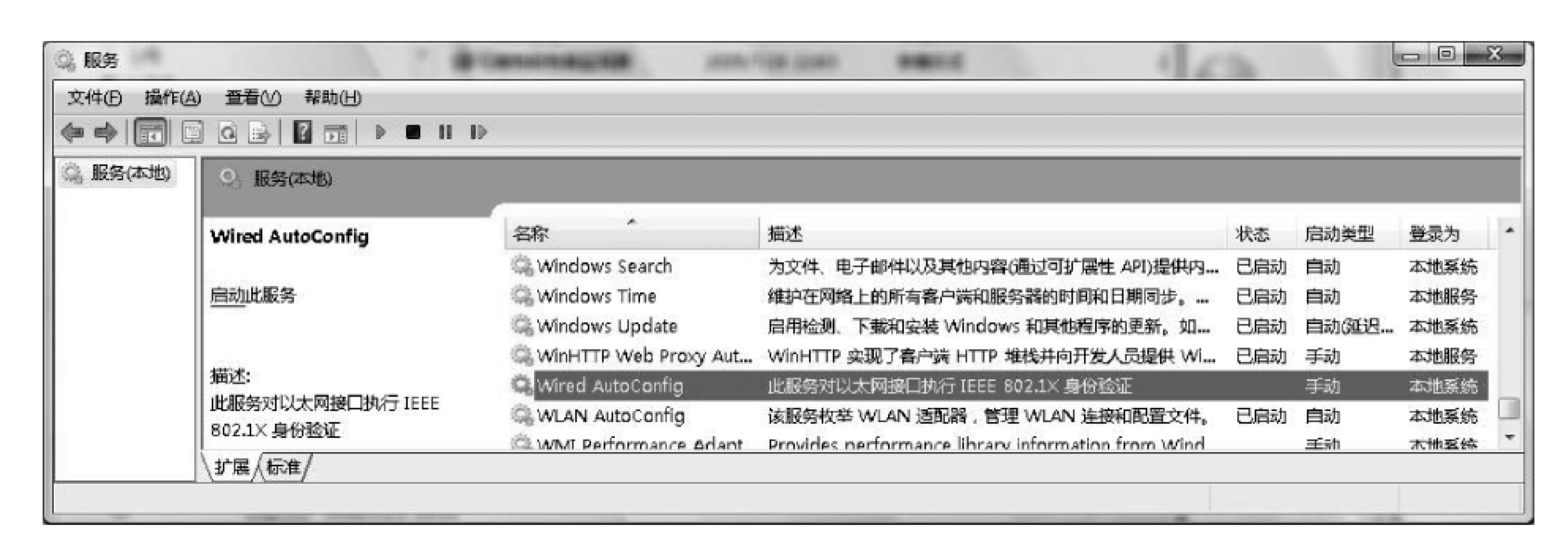


图 3-12　启用 Windows 系统上的 IEEE 802.1x 认证服务

在“选择网络身份验证方法”下拉列表框中选择身份验证方法，如图 3-13 所示，选择了“Microsoft：受保护的 EAP”作为身份验证方法。单击该下拉列表框右侧的“设置”按钮，在图 3-14 所示“受保护的 EAP 属性”对话框中对该验证方法进行详细配置。

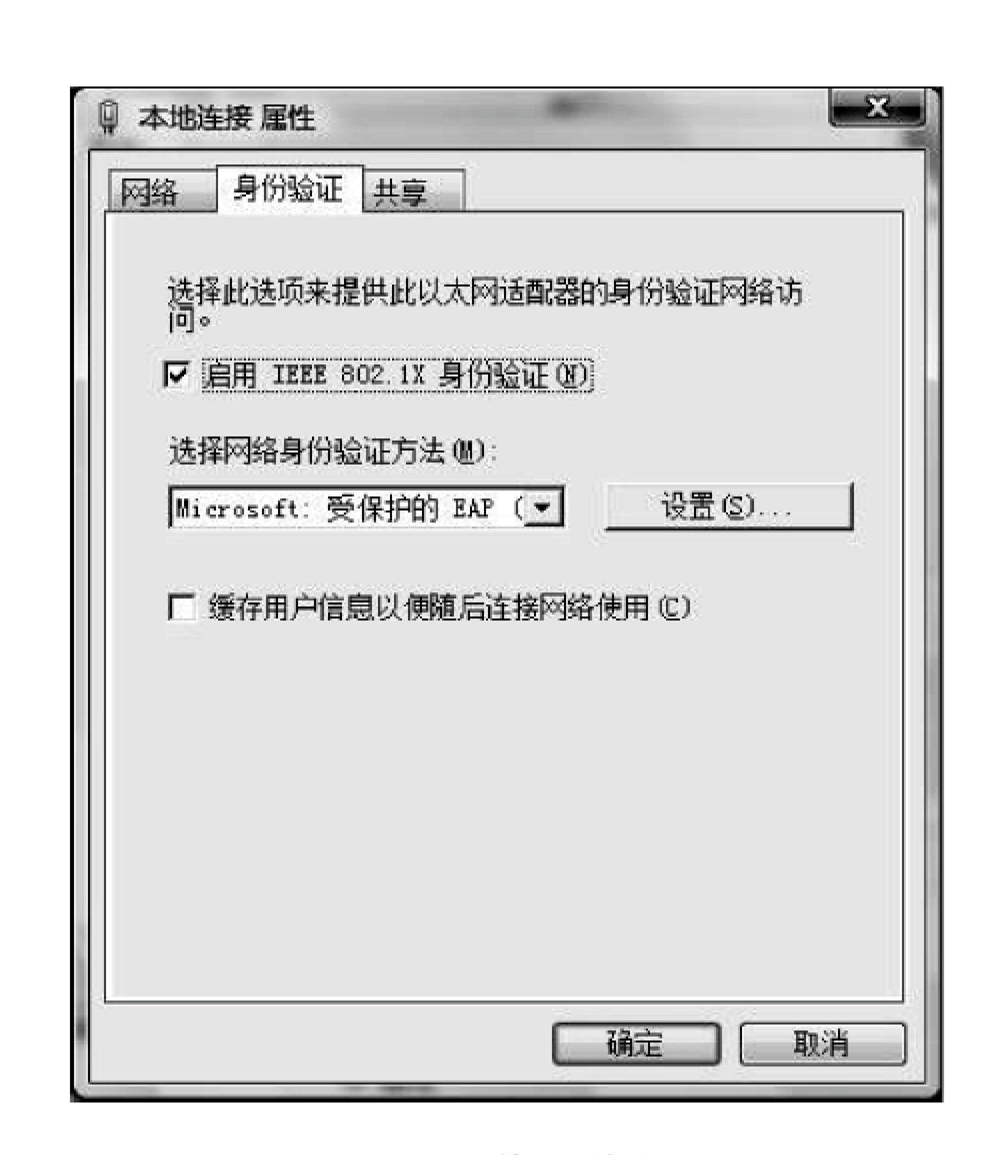


图 3-13　Windows 网络连接的 IEEE 802.1x 认证属性对话框



图 3-14　“受保护的 EAP 属性”对话框

在“选择身份验证方法”下拉列表框中选择“安全密码(EAP-MSCHAP v2)”身份验证方法。为使登录网络时系统能够弹出输入窗口，可单击其右侧的“配置”按钮，并在图 3-15 所示弹出的对话框中取消选择“自动使用 Windows 登录名和密码”复选框，单击“确定”按钮。



图 3-15　“EAP MSCHAPv2 属性”对话框

2. 在交换机上配置 IEEE 802.1x

在 Catalyst 交换机上配置 IEEE 802.1x 的步骤如表 3-13 所示，其中有关启用 AAA 并配置 RADIUS 服务器信息的操作命令参考 3.2.2 小节。

表 3-13 Catalyst 交换机 IEEE 802.1x 配置步骤

序号	操　作	相关命令	是否必要
步骤 1	启用 AAA，并配置 RADIUS 服务器有关信息	参见 3.2.2 小节	使用 RADIUS 方式时必要
步骤 2	定义 IEEE 802.1x 身份验证方法列表	aaa authentication dot1x	必要
步骤 3	启用交换机的 IEEE 802.1x 身份验证	dot1x system-auth-control	必要
步骤 4	配置端口启用 IEEE 802.1x 身份验证及相应参数	switchport mod access dot1x pae authenticator dot1x port-control	必要
步骤 5	检查、调试端口 IEEE 802.1x 身份验证配置	show dot1x debug dot1x all	可选

(1) 定义 IEEE 802.1x 身份验证方法列表

在 Cisco IOS 中，定义使用 IEEE 802.1x 进行身份验证的命令是在全局配置模式输入：

aaa authentication dot1x default ｛身份验证方式 ｛身份验证协议｝｝

其中，“身份验证方式”、“身份验证协议”等参数可参考 3.2.2 节中有关内容配置。

例如，使用 RADIUS 进行身份验证，则相应的配置命令为：

aaa authentication dot1x default group radius

(2) 全局启用 IEEE 802.1x 身份验证

在 Cisco IOS 中，定义启用 IEEE 802.1x 身份验证的命令是在全局配置模式输入：

dot1x system-auth-control

该命令在交换机上启用 IEEE 802.1x 方式的系统身份认证功能。

(3) 配置端口启用 IEEE 802.1x 身份验证及相应参数

除了要启用交换机上 IEEE 802.1x 方式的系统身份认证功能，还需指定交换机上哪些端口要进行 IEEE 802.1x 认证才可访问。

在 Cisco IOS 中，定义哪些端口启用 IEEE 802.1x 身份验证的命令是在端口配置模式输入：

dot1x port-control ｛ **auto** ｜ **force-authorized** ｜ **force-unauthorized** ｝

该命令中使用关键字 auto，则定义在当前端口上启用 IEEE 802.1x，并使端口根据交换机与客户端之间的 IEEE 802.1x 认证情况迁移到已授权或未授权状态。

若使用 force-authorized 关键字，则将在该端口上禁用 IEEE 802.1x，使端口不需要任何认证就迁移到已授权状态，该模式为端口的默认模式。

若使用 force-unauthorized 关键字，则强制端口迁移到未授权状态以拒绝所有该端口的访问，忽略客户端的所有认证请求，交换机不能通过该端口向客户端提供认证。

注意： 在配置端口 IEEE 802.1x 安全特性之前，一定要配置端口为接入模式，干道模式的端口不能使用 IEEE 802.1x。

在 Cisco IOS 中，定义端口为哪类 PAE 的命令是在端口配置模式输入：

dot1x pae authenticator

端口访问实体(Port Access Entity，PAE)是一个与某个端口相关联的支持 IEEE 802.1x 协议的逻辑实体。局域网端口可以充当身份验证者或申请者的角色，或者同时充当这两个角色。该命令定义端口作为身份验证者。

(4) 调试和检查交换机的 IEEE 802.1x 配置

在 Cisco IOS 中，检查端口 IEEE 802.1x 配置的命令是在特权配置模式输入：

show dot1x ｛ **all** ｜ **interface** ｛端口类型/编号｝｝

以输出端口 Fa0/22 IEEE 802.1x 配置为例，**show dot1x interface** 命令及输出如下。

```
Switch#show dot1x interface fa0/22
Dot1x Info for FastEthernet0/22
----------------------------
PAE                    = AUTHENTICATOR                    ①
PortControl            = AUTO                             ②
ControlDirection       = Both                             ③
HostMode               = SINGLE_HOST                      ④
ReAuthentication       = Disabled                         ⑤
QuietPeriod            = 60
ServerTimeout          = 30
SuppTimeout            = 30
ReAuthPeriod           = 3600 (Locally configured)        ⑥
ReAuthMax              = 2                                ⑦
MaxReq                 = 2
TxPeriod               = 30
RateLimitPeriod        = 0
```

其中：

① 表示该端口的 PAE 类型为身份验证提供者。

② 表示该端口控制模式配置为 AUTO，即启用 IEEE 802.1x 身份验证。

③ 表示该端口访问控制的方向为 Both，即对进出端口的流量都进行身份验证。

④ 表示该端口是否支持对多个主机的访问进行身份验证控制，SINGLE_HOST 即只支持单主机连接该端口，进行身份验证。

⑤ 表示是否支持重认证，Disabled 即不能。

⑥ 表示重认证时间间隔。

⑦ 表示最大的重认证次数。

在 Cisco IOS 中，调试交换机 IEEE 802.1x 配置的命令是在特权配置模式输入：

debug dot1x { **all** | **events** | }

其中，all 关键字将打开所有 IEEE 802.1x 调试信息；而关键字 events 将显示所有 IEEE 802.1x 事件信息。

3.3.3 模拟公司总部局域网 IEEE 802.1x 配置案例

模拟公司总部 2 号楼各部门均有一间以上会议室用于召开各类临时会议。由于这些会议室的网络接口所连接主机不固定，无法使用端口绑定 MAC 地址的方式防止非授权的访问，所以对于这些会议室所连接的接入交换机端口，需要通过配置 IEEE 802.1x 进行访问控制。各接入交换机端口 IEEE 802.1x 安全特性配置模板如下。

```
!
aaa new-model
aaa authentication dot1x default group radius
此处省略…
!
dot1x system-auth-control
此处省略…
!
interface FastEthernet0/22
switchport mode access
dot1x pae authenticator
dot1x port-control auto
此处省略…
!
radius-server host 200.100.8.30 auth-port 1812 acct-port 1813
radius-server key Net&Sec@sjzpc
!
```

本模板中会议室信息点对应接入交换机的端口为 FastEthernet0/22，在该端口上启用 IEEE 802.1x 安全特性，使用 RADIUS 服务器 200.100.8.30 进行远程认证。

3.4 交换机访问控制列表技术

3.4.1 交换机访问控制列表技术简介

访问控制列表作为网络安全中一种基本技术，在各层网络设备上都有应用，交换机也不会例外。在 Cisco Catalyst 三层交换机上，提供了如表 3-14 所示 4 种不同的访问控制列表技术。Cisco Catalyst 交换机会为每个数据包进行 4 次 ACL 查找：入站和出站安全 ACL 以及入站和出站 QoS ACL。

表 3-14 交换机访问控制列表技术

类 型	描 述	应 用
路由访问控制列表 RACL	Router Access Control List，在交换机三层接口上应用的访问控制列表技术，使用方法与第2章中介绍的常规访问控制列表技术相同	对交换机路由接口上通过的流量进行过滤。二层交换机不支持该功能
VLAN 访问控制列表 VACL	VLAN Access Control List，在交换机 VLAN 上应用的访问控制列表，也称 VLAN 访问映射表。支持对 Ethertype 和 MAC 地址的过滤	过滤某个 VLAN 内的非法流量。二层交换机不支持该功能
端口访问控制列表 PACL	Port Access Control List，在交换机二层端口上应用的访问控制列表，包括 IP 访问控制列表、MAC 访问控制列表等	提供端口级别颗粒度更细的网络安全访问控制
服务质量访问控制列表 QoS ACL	QoS Access Control List，用于指定 QoS 分类、标记、控制和调度应用于哪些数据流量	进行基于端口的流量控制及配合网络整体 QoS 配置实现

有关 RACL、QoS 参考本书第2章和第7章等有关内容。

1. VACL 实施技术细节

VACL 可以对三层交换机直连的同一个 VLAN 内的访问流量进行控制。例如限制同一 VLAN 内主机间互相访问、防止主机受本网络内网络蠕虫攻击等；也可以对其他网络访问本地网络的流量进行限制。

对于交换机上的 VLAN 而言，如果没有在 VLAN 虚接口上配置 RACL 或在 VLAN 上配置 VACL 来拒绝流量，那么流量默认就是被允许通过的。但是，一旦在 VLAN 上配置了 VACL，那么交换机就会对进入 VLAN 的流量进行匹配 VACL 的处理。

与常规 ACL 配置相同，VACL 中匹配条目的顺序非常重要，而且每个 VACL 最后都会自动隐含一条全部丢弃的条目。因此当流量进入配置有 VACL 的 VLAN 时，交换机将在 VACL 中顺序查找是否有匹配的条目。如果存在匹配条目，则按该条目后定义的操作进行处理；如果 VACL 中不存在匹配条目，则按最后隐含的条目将流量丢弃。

图 3-16 显示了在三层交换机上配置了 VACL 和 RACL 后，数据流量被处理的工作。从 PCa 发送给 PCb 的流量进入交换机后，首先进行 VLAN10 上配置的 VACL 检查，如果允许转发，则转发给 PCb；而从 PCa 发送给 PCc 的流量进入交换机后，除了进行 VLAN10 上配置的 VACL 检查，还需要在被路由到 PCc 所在 VLAN20 前，进行虚接口 VLAN10 上入方向的 RACL 检查、出方向的 RACL 检查，以及进入 VLAN20 后的 VACL 检查，才能转发给 PCc。

2. PACL 实施技术细节

PACL 可以在 Cisco 交换机的二层接入、干道或 EtherChannell 端口上配置，相对 VACL、RACL 提供更细的访问控制颗粒度。PACL 可以使用3种类型的访问控制列表：标准访问控制列表、扩展访问控制列表和 MAC 扩展访问控制列表。但是需要注意的是，标准访问控制列表、扩展访问控制列表只用于过滤 IP 分组，而 MAC 扩展访问控制列表只能过滤非 IP 分组，例如 ARP 报文。另外，如果在某端口上配置了 PACL，则该端口所属 VLAN 上配置的 VACL 会在该端口上失效。

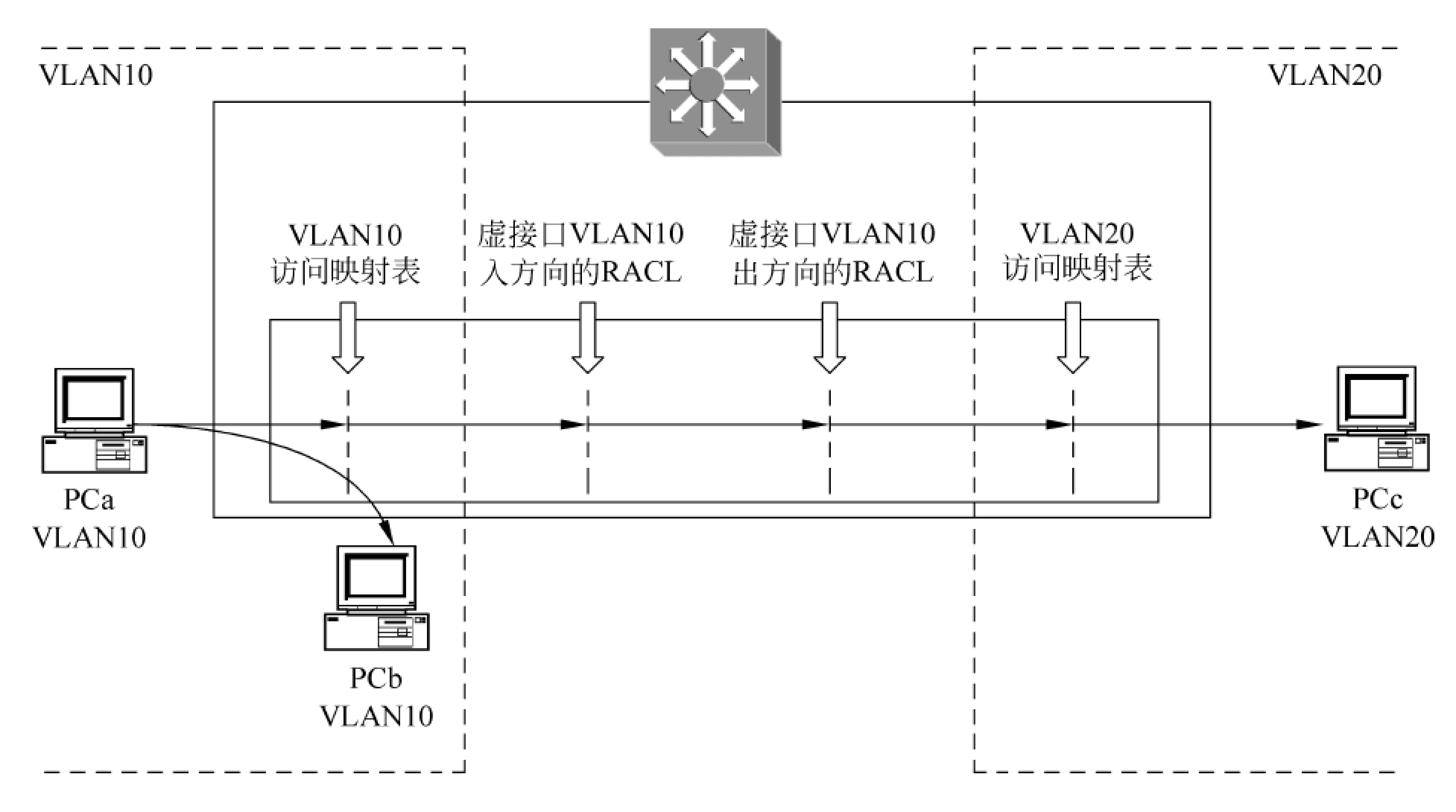


图 3-16 VACL、RACL 工作示例

3.4.2 配置 VACL

在 Cisco Catalyst 交换机上配置 VACL 的操作步骤与常规 ACL 一样，需要先定义一个 VLAN 访问映射表，指明匹配条件和相应操作，然后将其应用到相应 VLAN 上。其具体操作命令如表 3-15 所示。

表 3-15 VACL 配置步骤

步 骤	描 述	相关命令	
		基于 MAC 地址	基于 IP
步骤 1	定义 VACL 访问映射表要过滤的流量	mac access-list permit	ip access-list permit
步骤 2	定义 VLAN 访问映射表的名称和序号，并配置匹配条件、匹配后操作	vlan access-map match、action	
步骤 3	应用 VLAN 访问映射表	vlan filter	
步骤 4	检查调试 VLAN 访问映射表配置	show vlan access-map show vlan filter	

有关 ip access-list 命令的使用方法参见第 2 章常规 ACL 配置内容；有关 mac access-list 的配置内容参见 3.5.3 小节配置 PACL 部分。

1. 定义并应用 VLAN 访问映射表

Cisco IOS 上定义 VLAN 访问映射表的操作为在全局配置模式下输入：

vlan access-map ｛VLAN 访问映射表名｝［映射表条目编号］
 match ｛**ip address** ｛IP 访问控制列表标识｝ | **mac address** ｛MAC 扩展访问控制列表名｝｝
 action ｛**drop** | **forward**｝

该命令用于创建或修改一个 VLAN 访问映射表。其中“映射表条目编号”参数用于指定在映射表中插入条目的编号。

match、action 命令为 vlan access-map 命令的子句，需在 VLAN 访问映射表模式下输入。match 用于定义哪些 IP 或 MAC 流量需要被处理，action 用于定义符合条件的流量将被 drop(丢掉)还是 forward(转发)。需要注意的是，在访问控制列表中被 permit 的流量，才会匹配 match 子句后按照 action 子句定义的操作处理。

在 Cisco IOS 上，应用 VLAN 访问映射表的操作为在全局配置模式下输入：

vlan filter VLAN 映射表名 **vlan-list** vlan 号列表

其中，“vlan 号列表”参数可以输入多个以“,”分隔的 VLAN 编号。

注意：由于 VACL 应用在 VLAN 中所有流量上而不是应用接口或端口上，因此只需要指定 VACL 应用在哪些 VLAN 上，不需要指定 VACL 应用在 VLAN 哪个方向的流量上。

2. 检查及调试 VLAN 访问映射表

在 Cisco IOS 上，检查 VLAN 访问映射表配置的操作为在特权模式下输入：

show vlan access-map [VLAN 访问映射表名]

在 Cisco IOS 上，检查 VLAN 访问映射表应用情况的操作为在特权模式下输入：

show vlan filter [VLAN 访问映射表名 | **vlan** VLAN 标识]

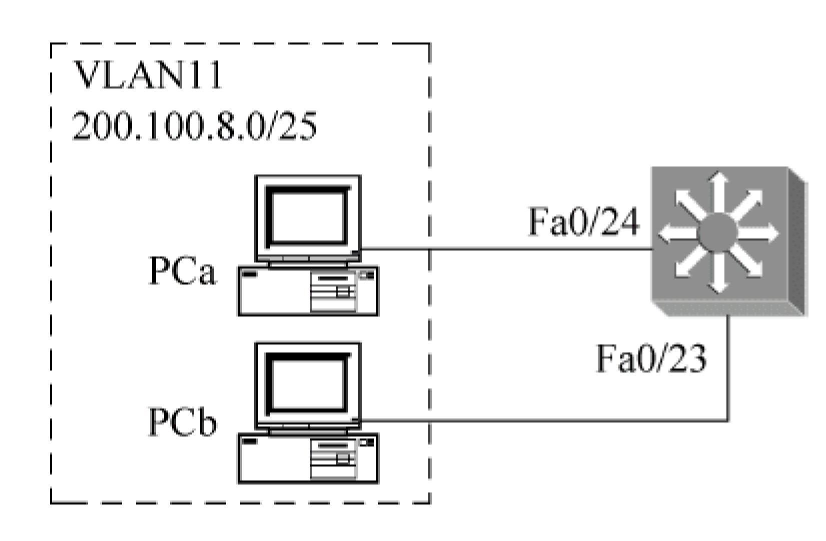


图 3-17　VACL 举例拓扑示意

3. VACL 配置举例

要禁止图 3-17 中 VLAN11 内主机对本网段的 HTTP 访问，则可以进行如下配置。

```
Switch(config)#interface range fa0/23 - 24                                    ①
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 11
Switch(config-if-range)#exit
Switch(config)#ip access-list extended ipacl-http                             ②
Switch(config-ext-nacl)#permit tcp 200.100.8.0 0.0.0.127 200.100.8.0 0.0.0.127 eq 80
Switch(config-ext-nacl)#exit
Switch(config)#ip access-list standard ipacl-any                              ③
Switch(config-std-nacl)#permit any
Switch(config-std-nacl)#exit
Switch(config)#vlan access-map vam-http 10                                    ④
Switch(config-access-map)#match ip address ipacl-http
Switch(config-access-map)#action drop
Switch(config-access-map)#exit
Switch(config)#vlan access-map vam-http 20                                    ⑤
Switch(config-access-map)#match ip address ipacl-any
```

```
Switch(config-access-map)#action  forward
Switch(config-access-map)#exit
Switch(config)#vlan  filter  vam-http  vlan-list  11                ⑥
Switch(config-access-map)#end
Switch#show  vlan  access-map                                       ⑦
Vlan access-map "vam-http"  10
  Match clauses:
    ip  address: ipacl-http
  Action:
    drop
Vlan access-map "vam-http"  20
  Match clauses:
    ip  address: ipacl-any
  Action:
    forward
Switch#show  vlan  filter                                           ⑧
VLAN Map vm-testhttp is filtering VLANs:
  11
```

其中：

① 按拓扑图要求将 Fa0/23 和 Fa0/24 端口配置为接入模式，并将其加入 VLAN11。

② 定义一个 IP 扩展访问控制列表 ipacl-http，该访问控制列表中只有一个条目，即允许所有访问网络 200.100.8.0/25 主机 HTTP 服务端口 80 的流量。

③ 定义一个标准 IP 访问控制列表 ipacl-any，该访问控制列表中只有一个条目，即允许所有 IP 流量。

④ 定义 VLAN 访问映射表条目 10，该条目将 ipacl-http 访问控制列表允许的流量全部丢弃。因此根据该 VLAN 访问映射表条目，则所有访问网络 200.100.8.0/25 主机 HTTP 服务端口 80 的流量将被丢弃。

⑤ 定义 VLAN 访问映射表条目 20，该条目将 ipacl-any 访问控制列表允许的流量全部转发。定义该条目的目的是防止其他流量被 VLAN 访问映射表中最末一条自动添加的丢弃操作丢弃。

⑥ 将 VLAN 访问映射表应用到 VLAN11 上。

⑦ 使用 show 命令显示 VLAN 访问映射表信息。输出信息中显示了所有已定义的 VLAN 访问映射表语句。

⑧ 使用 show 命令显示 VLAN 访问映射表应用情况，输出信息显示该访问映射表已经被应用到 VLAN11 上。

3.4.3 配置 PACL

PACL 配置中有关标准访问控制列表和扩展访问控制列表的定义、应用方法与第 2 章介绍的常规访问控制列表相同，此处不再赘述。

在 Cisco Catalyst 交换机上配置 MAC 扩展访问控制列表的步骤及命令如表 3-16 所示。

表 3-16　MAC ACL 配置步骤

步　骤	描　　述	有关命令	
		基于 MAC 地址的访问控制列表	基于 IP 的访问控制列表
步骤 1	定义 PACL 所需访问控制列表的名称和序号，并配置匹配条件和匹配后操作	**mac access-list、permit、deny**	**ip access-list permit、deny**
步骤 2	应用端口访问控制列表	**mac access-group**	**ip access-group**
步骤 3	检查调试端口访问控制列表配置	**show mac access-group**	**show ip access-list**
		show access-lists hardware counters	

有关 IP 访问控制列表定义及应用配置可参考第 2 章。

1. 定义并应用 MAC 扩展访问映射表

在 Cisco IOS 上，定义 MAC 扩展访问映射表的操作为在全局配置模式下输入：

mac access-list extended MAC 扩展访问控制列表名
permit ｛源 MAC 地址 源 MAC 地址通配符 ｜**any**｝｛目标 MAC 地址 目标 MAC 地址通配符 ｜ **any** ｜ **host** 源 MAC 地址｝［协议号 协议通配符］
deny ｛源 MAC 地址 源 MAC 地址通配符 ｜**any**｝｛目标 MAC 地址 目标 MAC 地址通配符 ｜ **any** ｜ **host** 源 MAC 地址｝［协议号 协议通配符］

其中，permit、deny 为 mac access-list 命令的子句，需在 MAC 扩展访问控制列表模式下输入。permit 子句定义允许哪些流量，deny 子句用于定义禁止哪些流量。permit、deny 子句中的 host 关键字用于定义来自某 MAC 地址的流量；any 关键字代指任何地址的流量。

在 permit、deny 子句中的“协议号”字段，用于定义允许或禁止哪种二层以上的协议流量。“协议号通配符”可以辅助“协议号”字段过滤多个协议。

在 Cisco IOS 上，在端口上应用 MAC 扩展访问映射表的操作为在端口配置模式下输入：

mac access-group MAC 扩展访问控制列表名 **in**

2. 检查及调试 PACL 配置

在 Cisco IOS 中，可以在特权用户模式下输入如下命令检查 MAC 扩展访问控制列表。

show mac access-group

该命令显示所有端口上应用的 MAC 扩展访问控制列表情况，其输出结果如下。

```
C3550-0-3-1#show mac access-group
Interface FastEthernet0/1:
   Inbound access-list is macl-pacl-arp
…
```

以上结果表示在端口 FastEthernet0/1 上应用了一个名为 macl-pacl-arp 的 MAC 扩

展访问控制列表。

3.4.4 模拟公司总部局域网交换机访问控制列表配置案例

在模拟公司总部局域网的交换机上配置访问控制，满足以下网络及信息安全要求。

（1）在各部网络中，市场部各主机间不能直接互访，但能与其他网络以及外网主机互访。

（2）各部网络内前 7 个 IP 由各部网络的网关、服务器使用。为防御蠕虫攻击，禁止到各网络内非网关、服务器主机的主动 TCP 连接请求和危险 UDP 端口的访问。

（3）为保护生产部网络内各系统安全，其他网络除能 ping 通生产主机外，不能与生产主机直接进行其他通信，只能通过生产部网络中的前置机间接获得生产数据，前置机 IP 范围是生产网络中的前 31 个 IP。

（4）限制各主机接入网络的 ARP 流量大小，在发现 ARP 洪水攻击的源主机后，使用 PACL 将其 ARP 流量过滤。

注意：此处访问控制列表配置未考虑第 2 章中所提及的访问控制要求。但在实际生产中，需整体考虑网络访问控制需求以设计安全策略模型。

根据现有网络拓扑、网络设备设备配置、网络性能和所支持的交换机访问控制列表功能，可参考以下方案分别配置各部网络所在汇聚、接入交换机，实现网络及信息安全要求。

（1）由于目前三层交换机才支持 VACL，而网络中在汇聚层才使用三层交换机，所以无法通过 VACL 过滤 VLAN 内主机间流量，因此只有在市场部网络所在接入交换机上配置基于 IP 扩展访问控制列表的 PACL，来限制该部网络 VLAN300 内各主机间互访，配置如下。

```
!
interface  FastEthernet0/24
 switchport  access  vlan  40
 switchport  mode  access
 ip  access-group  eacl-pacl-40  in                                        ①
!
ip  access-list  extended  eacl-pacl-40                                    ②
 permit  ip  any  200.100.10.0  0.0.0.7                                    ③
permit  tcp  any  200.100.10.0  0.0.0.127  established                     ④
 deny  tcp  any  200.100.10.0  0.0.0.127
 deny  udp  any  200.100.10.0  0.0.0.127  eq  netbios-ns                   ⑤
 permit  ip  200.100.10.0  0.0.0.7  any                                    ⑥
 permit  icmp  any  any                                                    ⑦
 deny  ip  200.100.10.0  0.0.0.127  200.100.10.0  0.0.0.127                ⑧
 permit  ip  any  any                                                      ⑨
!
```

其中：

① 在端口 Fa0/24 上应用名为 eacl-pacl-40 的 PACL。所有进入该端口的流量将被该 PACL 过滤。此处以在市场部网络所在接入交换机的接入端口 Fa0/24 为例，演示如

何使用 PACL 过滤流量。其中市场部网络 IP 地址为 200.100.10.0/25，VLAN 编号为 40。

② eacl-pacl-40 PACL 定义，该 PACL 使用扩展访问控制列表因为要对 TCP 浏览进行过滤。

③ 保证到达网络中服务器和网关等前 7 个 IP 地址的流量能正常通过。

④ 拒绝向本网段主机主动发起的 TCP 连接请求。

⑤ 拒绝到达本网段 UDP137 端口的流量通过。

⑥ 允许本网段中服务器和网关等前 7 个 IP 地址的流量。该访问控制条目用于允许服务器、网关响应主机的流量。

⑦ 允许所有 ICMP 流量通过。该条目允许用户使用 ping 命令来测试网络连通性。

⑧ 拒绝本网络中主机间互访。

⑨ 允许其他 IP 流量。该条目用于允许端口所连接主机访问其他网络。

(2) 在各接入交换机上配置基于 IP 扩展访问控制列表的 PACL，限制内网主机对本网段及总部其他网络内非服务器主机主动发起的 TCP 连接请求和 UDP 137 端口的请求，模拟公司研发部接入交换机访问控制配置举例如下。

```
!
interface FastEthernet0/9
 switchport access vlan 300
 switchport mode access
 ip access-group eacl-pacl-30 in
!
ip access-list extended eacl-pacl-300
 permit ip any 200.100.9.0 0.0.0.7
 permit tcp any 200.100.9.0 0.0.0.255 established
 deny tcp any 200.100.9.0 0.0.0.255
 deny udp any 200.100.9.0 0.0.0.255 eq netbios-ns
 permit ip any any
!
```

从研发部接入交换机访问控制配置可以看出，在研发部网络所在接入交换机的相应端口应用定义的 PACL；与市场部的 PACL 定义相比，研发部网络不需要限制网络内主机间的访问流量，因此，其 PACL 中可以省去禁止本网络主机间流量部分。

(3) 在生产部所在汇聚交换机上配置基于 IP 扩展访问控制列表的 VACL，允许其他网络对生产部网络的 ICMP 访问和对前置机的 IP 访问流量，拒绝对非前置机主机的访问流量。

(4) 发现 ARP 洪水攻击的源主机后，在相应交换机上配置 PACL 过滤该 MAC 地址的 ARP 流量，配置如下

```
!
vlan access-map vam-60 10                                    ①
 action forward
 match ip address eacl-vacl-60
vlan access-map vam-60 20                                    ②
```

```
 action   drop
 match   ip   address   sacl-vacl-60
vlan   filter   vam-60   vlan-list   60                                   ③
!
ip   access-list   standard   sacl-vacl-60                                ④
 permit   any
!
ip   access-list   extended   eacl-vacl-60                                ⑤
 permit   icmp   any   any
 permit   ip   any   200.100.11.0   0.0.0.31
 permit   ip   200.100.11.0   0.0.0.31   any
 permit   ip   200.100.11.0   0.0.0.255   200.100.11.0   0.0.0.255
!
```

其中：

① 定义 VLAN 访问映射表 vam-60 条目 10。该条目将转发匹配 eacl-vacl-60 的流量，即转发所有 VLAN600 中的 ICMP 流量、VLAN600 中的访问前置机以及前置机返回的流量、VLAN600 网络中主机互访的流量。

② 定义 VLAN 访问映射表 vam-60 条目 20。该条目将丢弃匹配 sacl-vacl-60 的流量，即丢弃来自所有主机的流量。

③ 在 VLAN600 上应用 VLAN 访问映射表。

④ 定义 IP 标准访问控制列表，允许来自所有主机的流量。

⑤ 定义 IP 扩展访问控制列表，允许所有 ICMP 流量，访问 VLAN600 中前置机的流量和 VLAN600 中返回的流量，以及 VLAN600 中主机互访的流量。

利用 MAC 访问控制列表禁止 ARP 流量配置举例如下。

```
!
mac   access-list   extended   macl-pacl-arp
 deny   host   0015.5886.bcec   any   0x806   0x0
!
interface   FastEthernet0/24
 switchport   access   vlan   300
 switchport   mode   access
此处省略...
 mac   access-group   macl-pacl-arp   in
```

其中：

- 定义名为 macl-pacl-arp 的 MAC 扩展访问控制列表。该例子显示如何在发现有大量来自 0015.5886.bcec 的 ARP 攻击流量时，通过 MAC 访问控制来限制流量。
- 该 MAC 扩展访问控制列表禁止来自 MAC 地址 0015.5886.bcec，类型为 0x806，类型通配符为 0 的流量，即 ARP 流量。
- 在该流量来源端口上应用名为 macl-pacl-arp 的 MAC 扩展访问控制列表，拒绝从来自 0015.5886.bcec 的流量从该端口进入交换机。

3.5　端口安全技术

3.5.1　端口安全技术简介

1. 端口安全技术产生的原因

防御局域网中 MAC 地址泛洪和 MAC 地址欺骗攻击是端口安全技术产生的主要原因。

（1）MAC 地址泛洪攻击

交换机一般会根据自己的 MAC 地址表转发数据帧，但如果在该表中找不到待转发数据帧的目的 MAC 地址，交换机就会将该数据帧在同一个网络中的所有端口上进行泛洪。“MAC 地址泛洪攻击”正是利用交换机这一工作原理而进行的。

交换机使用源地址学习方式来构建 MAC 地址表，但任何交换机的 MAC 地址表空间都是有限的，所以只要局域网中的恶意用户持续向交换机发送大量带有无效源 MAC 地址的数据帧，就会导致交换机 MAC 地址表空间的溢出。当交换机 MAC 地址表空间被大量无效 MAC 地址占满时，合法主机的 MAC 地址信息将再也无法加入到 MAC 地址表中。交换机不得不像一台集线器一样，将合法主机的流量泛洪到所有端口上，而恶意用户也就可以在其连接的交换机端口上，轻松截取网络中的所有数据流量。

（2）MAC 地址欺骗攻击

恶意用户监听网络上的数据流量，并从中获得网络上合法主机的 MAC 地址。然后使用 MAC 地址更改工具将自己的 MAC 地址伪装成网络上合法主机的 MAC 地址发送数据，以欺骗交换机学习到错误的 MAC 地址条目，这种攻击方式称为 MAC 地址欺骗攻击。MAC 地址欺骗攻击示意如图 3-18 所示。MAC 地址欺骗攻击常被恶意用户在进行中间人攻击时使用，目的是欺骗交换机将发往被攻击者的数据流量转发给自己；有些恶意用户也使用 MAC 地址欺骗来假冒已被授权的主机获得访问网络资源的权力。

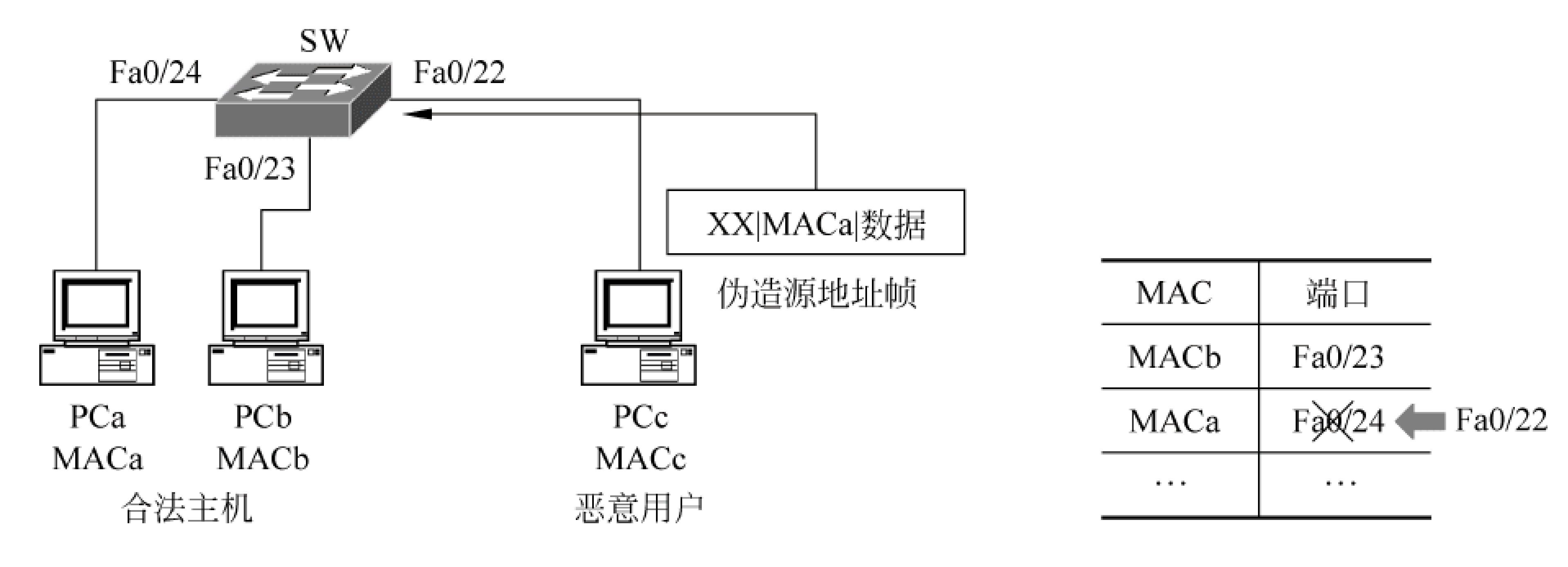


图 3-18　MAC 地址欺骗攻击示意图

2. 端口安全技术的主要内容

端口安全是一种基于 MAC 地址进行的二层安全技术，其工作原理是在交换机端口上允许或禁止来自某些 MAC 地址的流量进入。在一个安全端口已经分配了安全

MAC地址的情况下，所接收流量中的源地址如果与端口已定义安全MAC地址不符，则都会被拒绝进入交换机。以Catalyst交换机为例，其端口安全技术主要包括以下3个方面。

(1) MAC允许

MAC允许技术可以在交换机单个端口只允许来自某些MAC地址的数据流量通过，使用这种技术能保证单个端口的MAC地址条目不会占满整个MAC地址表空间，从而帮助交换机来抵御MAC地址泛洪攻击。同时由于启用端口安全特性的交换机不允许MAC地址表中出现不同端口对应同一个安全MAC地址的情况，所以这种技术手段也能帮助交换机抵御MAC地址欺骗攻击。

(2) 单播MAC过滤

单播MAC过滤是一种在特定VLAN上过滤掉指定源MAC地址流量的技术。由于只能对单播流量进行，所以被称为单播过滤。使用该技术可以过滤掉那些确定不会在某个VLAN出现的MAC地址，减少恶意用户攻击网络的机会。

(3) 阻塞单播、多播泛洪

这种端口安全技术可以配置在交换机单个端口上阻塞未知单播地址或多播地址的泛洪，防止未知单播、多播地址泛洪对安全端口的影响。

3. MAC允许技术实施技术细节

使用该技术手段需要了解两方面技术细节，即如何定义交换机端口的安全MAC地址和如何处理安全端口上发生的违背(Violation)安全规则行为(简称违规行为)。

(1) 定义交换机端口安全MAC地址的方式

可以使用以下3种方式在交换机端口上定义安全MAC地址。

① 手工配置端口对应的静态MAC地址。该地址将被储存在MAC地址表和配置中，交换机掉电后也不会丢失。

② 配置交换机端口能够学习的MAC地址数目。在这种方式下，交换机动态学习有限数目的安全MAC地址，这些MAC地址条目将一直保存在MAC地址表中，但不会保持在交换机配置文件中，因此掉电或重载后会被清除。

③ 配置交换机粘性获得安全MAC地址。在这种方式下，可以手工配置或者让交换机动态学习安全MAC地址，但学习到的安全MAC地址将被存储在配置文件中，交换机重新加载或断电时不会丢失。这种方式结合了以上两种方式的特性，可以解决在大型网络中手工配置安全MAC地址过于费时，而动态学习安全MAC地址又不能保证交换机掉电后重新学到的MAC地址来自合法主机的问题。

交换机默认不会清除MAC地址表中的安全MAC地址条目，直到掉电或重载。但可以为端口配置老化机制，让交换机在一定时间后自动清除端口上的安全MAC条目。

- 绝对状态机制：端口上的安全地址会在指定时间后被清除，这是Catalyst交换机默认使用的老化机制。
- 休止状态机制：端口上的安全地址会在指定的闲置时间后被清除。

（2）违背安全规则行为的处理方式

出现以下两种情况之一，则交换机将视为发生违规行为。

① 交换机端口上收到与已定义安全 MAC 地址不符的源 MAC 地址数据流量。

② 交换机端口动态学习安全 MAC 地址过程中收到与另一端口已定义为安全 MAC 地址相同的源 MAC 地址流量。

交换机处理违背安全规则行为的模式有以下 3 种。

① 保护模式(protect)。端口使用该种模式，交换机将丢弃所有未知源 MAC 地址的单播或组播流量，并且不会发出任何通知。

② 限制模式(restrict)。对于动态学习安全 MAC 地址的端口，如果使用该种模式，交换机会在安全 MAC 地址条目数达到了设置限度时，丢弃未知源 MAC 地址的流量，发出违规通知，并发出一个 SNMP 陷阱记录一个日志消息，且违规行为计数器递增。这种状态将一直持续到安全 MAC 地址数量低于设置限度才可以解除。

③ 关闭模式(shutdown)。使用该种模式的端口，会在发生违规行为后处于错误禁用(err-disable)状态，端口 LED 关闭，并发出一个 SNMP 陷阱记录一个日志消息，且违规计数器递增。这是安全端口默认的违规行为模式。端口一旦处于错误禁用状态，将一直持续到交换机掉电重启，或者由网管员手工解除这种状态才能恢复。

4．单播、多播泛洪阻塞实施技术细节

对于配置了端口安全的交换机端口而言，当这些端口在 MAC 地址表中已有对应安全 MAC 地址条目时，向这些端口的泛洪就是不必要的。网络末梢上不必要的 MAC 泛洪如图 3-19 所示，图中所有 PC 都会丢弃交换机发出的 MAC 泛洪，而交换机此时发出的泛洪会让同一个 VLAN 中的所有设备都承担不必要的流量。因此作为 MAC 允许等端口安全技术的一个必要辅助技术，在已定义了安全 MAC 地址的安全端口上配置单播、多播阻塞，会有效降低不必要泛洪对主机工作效率的影响。

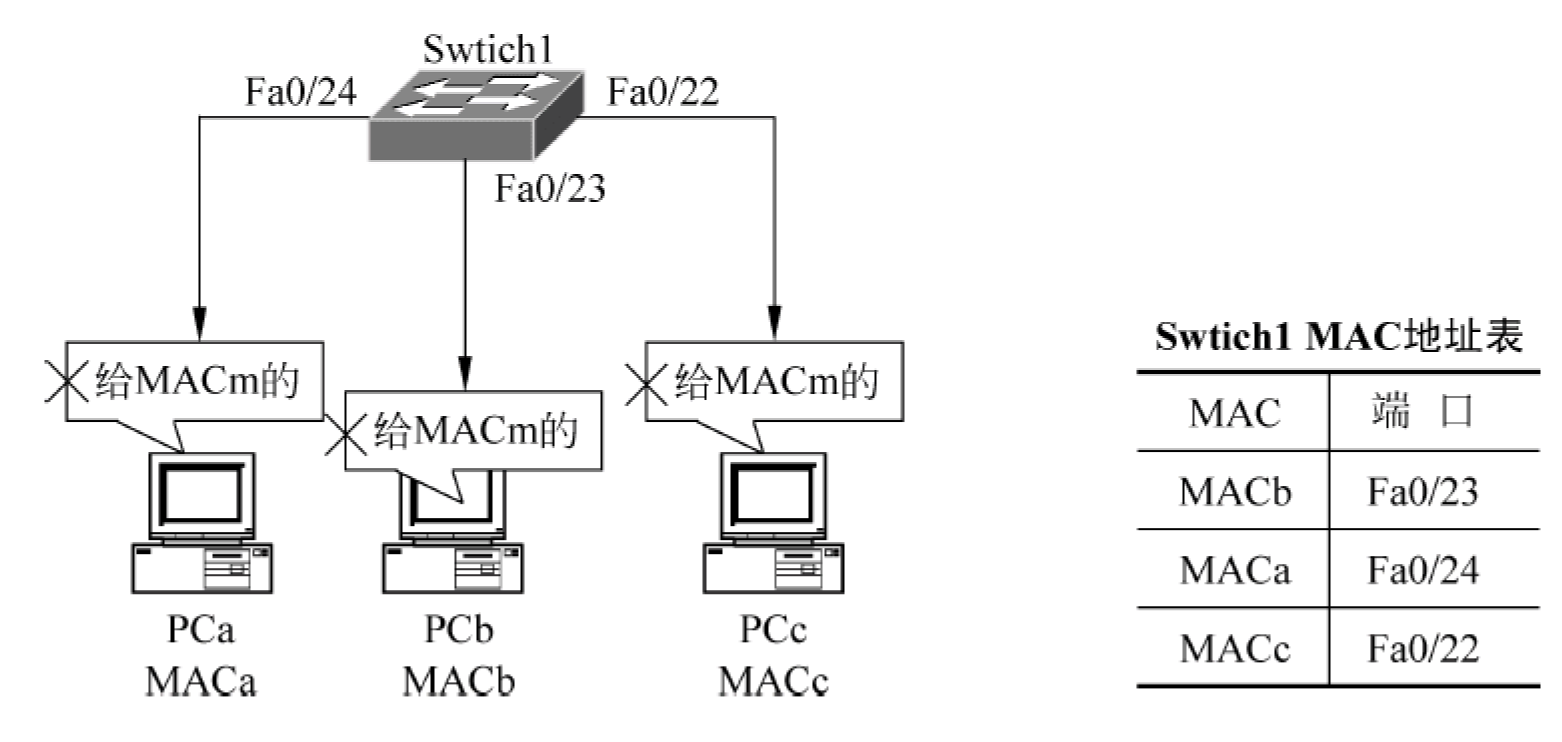


图 3-19　网络末梢上不必要的 MAC 泛洪

3.5.2　交换机端口安全配置方法

1．启用端口安全以及配置 MAC 允许

在 Catalyst 交换机上配置允许源 MAC 地址流量端口安全的步骤及相应命令如表 3-17 所示。

表 3-17 允许源 MAC 地址流量端口安全的配置步骤及命令

序号	配　　置	有 关 命 令	是否必须
步骤 1	在端口启用端口安全特性	**switchport mode access** **switchport port-security**	是
步骤 2	配置交换机静态安全 MAC 地址或者动态学习的安全 MAC 地址数量限度	**switchport port-security mac-address** **switchport port-security maximum** **switchport port-security mac-address sticky**	任选一个
步骤 3	指定交换机端口的安全违规行为模式及相应参数	**switchport port-security violation** **errdisable recovery cause psecure-violation** **errdisable recovery interval**	可选
步骤 4	配置交换机端口安全 MAC 地址老化参数	**switchport port-security aging**	可选

(1) 在端口启用端口安全特性

在 Cisco IOS 中，在端口启用端口安全特性的命令为在端口配置模式下输入：

switchport port-security

注意： Catalyst 交换机端口的默认工作模式为 auto，当端口处于自动协商模式时，启用端口安全特性会报错 Command rejected: FastEthernet0/24 is a dynamic port.，因此一定要在启用端口安全特性前使用 **switchport mode access** 命令明确指定端口模式为接入(access)模式，trunk 模式的端口不能配置端口安全特性。

(2) 配置交换机静态安全 MAC 地址或者动态学习安全 MAC 地址最大数目

在 Cisco IOS 中，手工配置端口静态安全 MAC 地址的命令为在端口配置模式下输入：

switchport port-security mac-address { 安全 MAC 地址 }

在 Cisco IOS 中，配置动态学习安全 MAC 地址的命令为在端口配置模式下输入：

switchport port-security maximum {安全 MAC 地址条目最大数 }

其中，参数“安全 MAC 地址条目最大数”默认为 1。

在 Cisco IOS 中，配置粘性安全 MAC 地址的命令为在端口配置模式下输入：

switchport port-security mac-address sticky

在配置动态学习安全 MAC 地址的最大地址条目数时，需要根据企业信息点数量和交换机 MAC 地址空间情况进行合理规划。例如，可将所有主机接入端口的安全 MAC 地址条目最大数设置为 1，并将剩余安全 MAC 地址条目空间按需分配给下联其他交换机的端口。

例如，对图 3-20 所示网络中交换机配置端口安全，交换机 Switch1 和交换机 Switch2 处于同一个网络中；交换机 Switch2 为接入交换机，连接一个办公网络，且所接入主机不固定，但不允许再有其他网络设备接入该交换机；交换机 Switch1 端口 Fa0/24 下联交换机 Switch2，其端口 Fa0/22 固定连接主机 PCc。

根据以上条件不难看出，交换机 Switch2 所有主机接入端口上可以配置动态获得安全 MAC 地址，且动态获得安全 MAC 地址的最大数目为 1；由于接入交换机 Switch2 的主机最

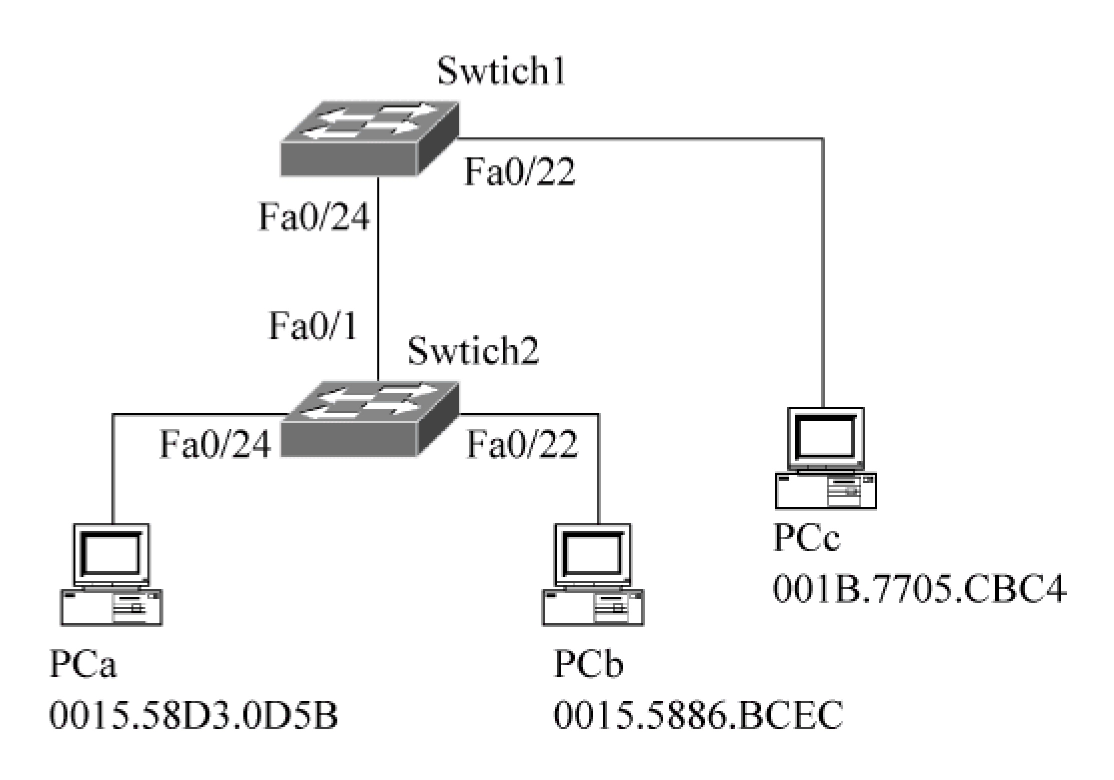


图 3-20　端口安全示例拓扑

终都要接入交换机 Switch1 的下联端口 Fa0/24，所以若要为 Fa0/24 端口配置动态安全 MAC 地址，则需要更大的安全 MAC 地址条目数，例如 48 个。同时交换机 Switch1 的 Fa0/22 端口需要静态指定安全 MAC 地址，或者使用粘性方式获得安全 MAC 地址。

（3）指定交换机端口的安全违规行为模式及相应参数

在 Cisco IOS 中，手工配置端口安全违规行为模式的命令为在端口模式下输入：

switchport　port-security　violation ｛ **protect** ｜ **restrict** ｜ **shutdown** ｝

其中，protect、restrict、shutdown 则为"保护"、"限制"、"关闭"3 种违规模式，shutdown 为默认安全违规模式。

选择哪种违规模式取决于端口性质，如果端口接入的是服务器，则应选择"限制"模式，以保护网络服务不受违规行为的影响；如果端口接入的是普通主机，则应选择"关闭"模式，并指定相应的 err-disable 计时器，这样可以在发生违规行为时，不需要网管员手工干预就可以重新建立连接。

err-disable 计时器是一个全局选项，对于任何配置为关闭模式的端口有效。在 Cisco IOS 中，配置 err-disable 计时器的命令为在全局配置模式下输入：

errdisable　recovery　cause　psecure-violation
errdisable　recovery　interval ｛ 违规后端口关闭秒数 ｝

第一行为打开端口安全关闭模式的 err-disable 计时器。

第二行为配置端口发生违规行为后多久可以重新启用。单位为秒，数值范围为 30～86400，默认值为 300。

以图 3-20 为例，交换机 Switch1 上有关的端口安全配置如下。

```
errdisable   recovery   cause   psecure-violation                ①
errdisable   recovery   interval   400                           ②
!
interface   FastEthernet0/22
 switchport   mode   access                                      ③
switchport   port-security                                       ④
 switchport   port-security   violation restrict                 ⑤
```

```
 switchport  port-security  mac-address  0015.5886.bcec                    ⑥
!
interface  FastEthernet0/24
 switchport  mode  access
switchport  port-security
 switchport  port-security  maximum 48                                     ⑦
!
```

其中：

① 打开 errdisable 计时器。

② errdisable 计时器间隔配置为 400 秒。

③ 配置端口模式为接入模式。

④ 启用端口安全特性。

⑤ 配置违规行为模式为限制模式。

⑥ 配置端口静态安全 MAC 地址为 0015.5886.bcec。

⑦ 配置 Fa0/24 端口动态安全 MAC 地址条目最大数为 48 个。

注意使用默认关闭模式作为违规行为模式，所以配置文件中未显示违规行为配置。

以图 3-20 为例，交换机“Switch2”上有关的端口安全配置如下。

```
errdisable  recovery  cause  psecure-violation                             ①
…
interface  FastEthernet0/23
 switchport  mode  access
 switchport  port-security
 switchport  port-security  mac-address  sticky                            ②
!
interface  FastEthernet0/24
 switchport  mode  access
 switchport  port-security
!                                                                          ③
```

其中：

① 打开 errdisable 计时器。注意这里使用默认 300 秒作为 errdisable 计时器间隔，所以在配置文件中不会显示 errdisable 计时器间隔配置命令。

② 端口 Fa0/23 被配置为使用粘性。

③ 动态获得安全 MAC 地址，且最大数为 1，违规行为模式是关闭模式，这些配置是端口安全 MAC 地址的默认配置，所以配置文件中不会显示这些配置命令。

（4）配置交换机端口安全 MAC 地址老化参数

在 Cisco IOS 中，配置交换机端口安全 MAC 地址老化参数的命令分别为在端口模式下输入：

```
switchport  port-security  aging  static                                   ①
switchport  port-security  aging  time  { 老化时间 }                        ②
switchport  port-security  aging  type  { absolute | inactivity }          ③
```

命令说明如下。

① 该命令用于启用对静态安全 MAC 地址的老化。

② 该命令用于设置老化时间,单位为分钟,范围为 1～1440。当老化机制类型设置为绝对老化机制时,该时间为端口获得安全 MAC 地址开始算起到达被清除的时间,而如果老化机制类型设置为休止状态机制,则该时间为从端口上一次接收到某安全 MAC 地址数据流量算起。

③ 该命令用于设置老化机制类型,关键字 absolute 为绝对老化机制,关键字 inactivity 为休止状态机制。

2. 配置单播 MAC 过滤和阻塞单播、多播泛洪

(1) 配置单播 MAC 过滤

虽然本书将单播过滤放在端口安全部分介绍,但在 Catalyst 交换机上,单播过滤的配置却是基于 VLAN 进行的。在 Cisco IOS 中,配置单播过滤的命令为在全局配置模式下输入:

mac-address-table　static　{被过滤的源 MAC 地址}　**vlan**　{VLAN 号}　**drop**

例如,一般正常网络流量的源 MAC 地址不会为 0000.0000.0000,所以可在网络中过滤来自该 MAC 地址的流量。对于一个只有 VLAN1 的 Catalyst 接入交换机而言,相应的配置命令为:

mac-address-table　static　0000.0000.0000　vlan　1　drop

(2) 配置阻塞单播、多播泛洪

在 Cisco IOS 中,阻塞单播、多播泛洪的命令为在端口配置模式下输入:

switchport　block　{　**multicast**　|　**unicast**　}

其中,使用 multicast 关键字即为阻塞多播,使用 unicast 即为阻塞单播。

3. 检查、调试端口安全配置

完成端口安全的配置后需检查和调试配置,或在网络运行中发现可能由端口安全配置导致的故障时,在 Cisco IOS 中,可以使用相应命令对端口安全配置进行调试和检查。

(1) 端口安全配置调试

在 Cisco IOS 中,在特权模式输入以下命令来打开端口安全调试功能。

debug　port-security

仍以图 3-20 中交换机 Switch2 为例,打开其端口调试功能,并在其 Fa0/24 端口接入另一交换机 Switch3,同时 Switch3 上接有两台计算机 PCd、PCe,此时在交换机 Switch2 上使用 debug　port-security 命令输出如下。

```
00:53:18: PSECURE: psecure_vp_list_fwdchange invoked
00:53:20: PSECURE: Read:0, Write:1
00:53:20: PSECURE: swidb = FastEthernet0/24 mac_addr = 0015.5886.bcec vlanid = 1
00:53:20: PSECURE: Adding 0015.5886.bcec as dynamic on port Fa0/24 for vlan 1
00:53:20: PSECURE: Adding address vlan 1 0015.5886.bcec to port-security
```

```
00:53:20：PSECURE：Adding addresses to port-security sub block
...
00:58:15：PSECURE：Read:1，Write:2
00:58:15：PSECURE：swidb = FastEthernet0/24 mac_addr = 0015.58d3.0d5b vlanid = 1
00:58:15：PSECURE：Adding 0015.58d3.0d5b as dynamic on port Fa0/24 for vlan 1
00:58:15：PSECURE：Violation/duplicate detected upon receiving 0015.58d3.0d5b on vlan 1：port_num_addrs 1 port_max_addrs 1 vlan_addr_ct 1：vlan_addr_max 1 total_addrs 0：max_total_addrs 8192
00:58:15：PSECURE：psecure_add_addr_check：Security violation occurred，bring down the interface
00:58:15：%PM-4-ERR_DISABLE：psecure-violation error detected on Fa0/24，putting Fa0/24 in err-disable state
00:58:15：PSECURE：psecure_vp_fwdchange invoked
00:58:15：PSECURE：psecure_vp_linkdown port Fa0/24，vlan 1，oper mode access，sb mode access
00:58:15：PSECURE：Clearing HA table for 1
00:58:15：PSECURE：psecure_clear_ha_table：called
00:58:15：PSECURE：psecure_clear_ha_table：delete 0015.5886.bcec vlan 1
00:58:15：PSECURE：psecure_linkchange：Fa0/24   hwidb=0x181D068
00:58:15：PSECURE：Link is going down
00:58:15：PSECURE：psecure_linkdown_init：Fa0/24 hwidb = 0x181D068
00:58:15：PSECURE：psecure_deactivate_port_security：Deactivating port-security feature
00:58:15：PSECURE：port_deactivate：port status is 0
00:58:15：PSECURE：psecure_clear_ha_table：called
00:58:15：%PORT_SECURITY-2-PSECURE_VIOLATION：Security violation occurred，caused by MAC address 0015.58d3.0d5b on port FastEthernet0/24.
00:58:15：PSECURE：Security violation，TrapCount:1
00:58:15：PSECURE：psecure_vp_notfwd_msg_handler invoked
00:58:16：%LINEPROTO-5-UPDOWN：Line protocol on Interface FastEthernet0/24，changed state to down
00:58:16：%LINEPROTO-5-UPDOWN：Line protocol on Interface Vlan1，changed state to down
00:58:17：%LINK-3-UPDOWN：Interface FastEthernet0/24，changed state to down
...
01:06:50：%PM-4-ERR_RECOVER：Attempting to recover from psecure-violation err-disable state on Fa0/24
01:06:52：PSECURE：psecure_linkchange：Fa0/24   hwidb=0x181D068
01:06:52：PSECURE：Link is coming up
01:06:52：PSECURE：psecure_linkup_init：Fa0/24 hwidb = 0x181D068
01:06:52：PSECURE：psecure_vp_linkup port Fa0/24，vlan 1，mode access
01:06:52：PSECURE：psecure_vp_linkup Populating addresses for vlan 1
01:06:52：PSECURE：psecure_activate_port_security：Activating port-security feature
01:06:52：PSECURE：port_activate：status is 1
01:06:52：PSECURE：psecure_clear_ha_table：called
01:06:52：PSECURE：psecure_activate_port_security：Deleting all dynamic addresses from h/w tables.
01:06:52：PSECURE：psecure_platform_delete_all_addrs：deleting all addresses on vlan 1
01:06:54：%LINK-3-UPDOWN：Interface FastEthernet0/24，changed state to up
01:06:55：%LINEPROTO-5-UPDOWN：Line protocol on Interface FastEthernet0/24，changed state to up
```

其中：

Adding 0015.5886.bcec as dynamic on port Fa0/24 for vlan 1 表示 在 Switch3 的 PCd 上 ping PCa，此时 PCd 的 MAC 地址 0015.5886.bcec 被 Switch2 学习到。

swidb = FastEthernet0/24 mac_addr = 0015.58d3.0d5b vlanid = 1 表示在 Switch3 的 PCe 上 ping PCa，此时带有 PCd 源 MAC 地址 0015.58d3.0d5b 的帧被 Switch2 接收。

psecure-violation error detected on Fa0/24, putting Fa0/24 in err-disable state 表示由于 Switch2 Fa0/24 端口安全配置只允许 1 个安全 MAC，所以该端口被置于 err-disable 状态。

Line protocol on Interface FastEthernet0/24, changed state to down 表示由于 Switch2 Fa0/24 端口安全配置使用默认的违规行为模式，即关闭模式，所以 Fa0/24 端口将被 shutdown。

Attempting to recover from psecure-violation err-disable state on Fa0/24 表示由于 Switch2 上启用了默认 err-disable 计时器，所以经一段时间后，Fa0/24 端口的 err-disable 状态被自动清除。

Line protocol on Interface FastEthernet0/24, changed state to up 表示 Fa0/24 端口被重新启用。

(2) 检查端口安全 MAC 地址表

在 Cisco IOS 中，可以在特权模式下输入以下命令来检查端口安全配置情况。

show port-security { **address** [**vlan**] | **interface** { 端口 ID } }

其中，address 关键字用于查看安全 MAC 地址表内容，以图 3-20 中交换机 Switch2 为例，使用 show port-security address 命令输出信息如下。

```
Secure Mac Address Table
---------------------------------------------------
Vlan    Mac Address       Type              Ports     Remaining Age            ①
                                                         (mins)
----    ---------         ----              -------   ----------
 1      0015.5886.bcec    SecureDynamic     Fa0/24    < 1                      ②
---------------------------------------------------
Total Addresses in System (excluding one mac per port)      : 0                ③
Max Addresses limit in System (excluding one mac per port) : 8192              ④
```

以上各行操作含义如下。

① 显示端口安全地址信息命令的信息内容包括 5 项内容，即 Vlan(安全 MAC 地址所属 VLAN)、Mac Address(安全 MAC 地址)、Type(安全 MAC 地址类型)、Ports(该安全 MAC 地址来源端口)、Remaining Age(该安全 MAC 地址的剩余老化时间)。

② 目前仅有 1 条安全 MAC 地址信息。该安全 MAC 地址属于 VLAN1，地址为 0015.5886.bcec，该安全 MAC 地址是动态学习获得的安全 MAC 地址，来源端口是 Fa0/24，该安全 MAC 地址设置了老化机制，剩余时间小于 1 分钟。

③ 目前系统中所有安全 MAC 地址数量，除每个端口 1 个安全 MAC 地址，总数为 0。

④ 目前系统中安全 MAC 地址数限制，除每个端口 1 个安全 MAC 地址，最大数

为 8192。

以图 3-20 中交换机 Switch2 为例，使用 show port-security interface 命令输出信息及解释如下。

```
Port Security                  : Enabled                 ①
Port Status                    : Secure-up               ②
Violation Mode                 : Shutdown                ③
Aging Time                     : 1 mins                  ④
Aging Type                     : Absolute                ⑤
SecureStatic Address Aging     : Disabled                ⑥
Maximum MAC Addresses          : 1                       ⑦
Total MAC Addresses            : 1                       ⑧
Configured MAC Addresses       : 0                       ⑨
Sticky MAC Addresses           : 0                       ⑩
Last Source Address:Vlan       : 0015.5886.bcec:1        ⑪
Security Violation Count       : 0                       ⑫
```

其中：

① 该端口是否启用了端口安全，Enabled 表示已经启用。

② 该端口目前状态，Secure-up 表示该端口为安全端口，且处于可用状态。

③ 该端口的违规模式配置，Shutdown 表示为关闭模式。

④ 该端口的老化时间，0 mins 表示目前没有配置老化时间。

⑤ 该端口的老化机制类型，Absolute 表示目前使用绝对老化机制。

⑥ 该端口是否启用了老化机制，Disabled 表示目前没有启用老化机制。

⑦ 该端口配置的安全 MAC 地址最大数目，目前值为 1，表示最多只能有 1 个安全 MAC 地址。

⑧ 该端口已有安全 MAC 地址数，目前值为 1，表示目前只有安全 MAC 地址。

⑨ 该端口静态配置的安全 MAC 地址数，目前值为 0，表示目前没有配置静态安全 MAC 地址。

⑩ 该端口使用粘性方式获得安全 MAC 地址数，目前值为 0，表示还没有使用该方法获得的安全 MAC 地址。

⑪ 该端口上一次获得的源 MAC 地址及所属 VLAN，目前值为 0015.5886.bcec:1。

⑫ 该端口违规行为计数器，目前值为 0，表示该端口还未发生过安全违规行为。

3.5.3 模拟公司总部局域网端口安全配置案例

根据模拟公司总部局域网安全任务要求，可为模拟公司总部局域网内交换机设计如下端口安全配置方案。

(1) 各接入交换机“C2960-0-楼号-设备号”端口安全特性配置如下，表 3-18 为配置列表。

接入交换机物理位置分散，直接连接用户主机，最易受到 MAC 地址欺骗、泛洪攻击，因此在各接入交换机的接入端口上均启用端口安全特性。

表 3-18　模拟公司总部局域网接入交换机端口安全配置列表

网络	行政管理部	研发部	网络中心	市场、售后部	生产部
端口类型	接入				
是否安全端口	是				
地址学习方式	粘性	动态	粘性	动态	粘性
MAC 数目限制	1				
违规模式	restrict	shutdown	restrict	shutdown	restrict
启用 err-disable 计时	否	是	否	是	否
err-disable 间隔/秒		300		300	
老化机制		启用		启用	
老化类型		休止		休止	
老化时间/分钟		3		3	
单播 MAC 过滤	0000.0000.0000	0000.0000.0000	0000.0000.0000	0000.0000.0000	0000.0000.0000
阻塞单播、多播泛洪	阻塞				

研发、市场、售后等部网络内有大量移动设备，因此其接入交换机安全端口适合选用动态学习安全 MAC 地址方式；而网络中心、管理、生产等部不应出现大量移动设备，因此其接入交换机安全端口适合选用粘性学习安全 MAC 地址方式。

为保证接入交换机各安全端口不会接入未经授权的交换机、集线器，各接入交换机安全端口的安全 MAC 地址数目限制为 1 个。

网络中心、生产部网络要提供网络服务，因此其接入交换机安全端口应配置为限制违规模式，以保证违规行为发生时不会中断网络服务。管理部要求保持网络连接最大可靠性，因此其接入交换机安全端口也应配置为限制违规模式，以保证违规行为发生时不会中断网络连接。研发、市场、售后等部网络在保证网络接入灵活性同时安全风险更大，适宜采用关闭违规模式，提高网络安全系数。

在配置了安全端口关闭违规模式的交换机上启用 err-disable 计时器可以在指定时间间隔内清除端口的 err-disable 状态，使关闭的端口不需网管员干预就可以再次启用，因此适合于研发、市场、售后等部网络内接入交换机。但 err-disable 计时器不能清除配置文件中的粘滞安全 MAC 地址，因此不适于管理部、网络中心、生产部等网络中的接入交换机。

除全 0 MAC 地址外，各部网络中不应出现的 MAC 地址可根据实际情况设置。

由于各部接入交换机均设置了安全端口，因此应配置单播、多播泛洪阻塞减少不必要的流量。

注意：由于网络中所有设备都应是可管理的，所以网络中所有交换机上联端口都需配置为干道(trunk)模式以允许管理 VLAN 和业务 VLAN 流量通过，因此以上列表中只在各交换机接入端口上实施端口安全配置。

(2) 由于各汇聚交换机、核心交换机的端口都工作在干道模式，且这些设备位置分布相对集中，恶意用户直接连接到这些端口进行 MAC 欺骗、泛洪攻击的可能性较小，因此对这些端口不再配置端口安全。

3.6 DHCP 监听、IP 源防护与 ARP 检测技术

3.6.1 DHCP 攻击及 DHCP 监听技术简介

1. DHCP 攻击

目前针对 DHCP 协议进行的攻击主要有以下两种类型。

（1）对 DHCP 服务器进行的 DoS 拒绝服务攻击

如图 3-21 所示，利用 DHCP 服务器不对 DHCP 客户端进行验证就响应其 DHCP 请求并分配 IP 地址的这一安全漏洞，恶意用户只要在网络上广播大量含有不同伪造 MAC 地址的 DHCP 请求报文，就可以很快耗尽 DHCP 服务器地址池中有限的 IP 地址资源，导致 DHCP 服务器不能继续提供服务。

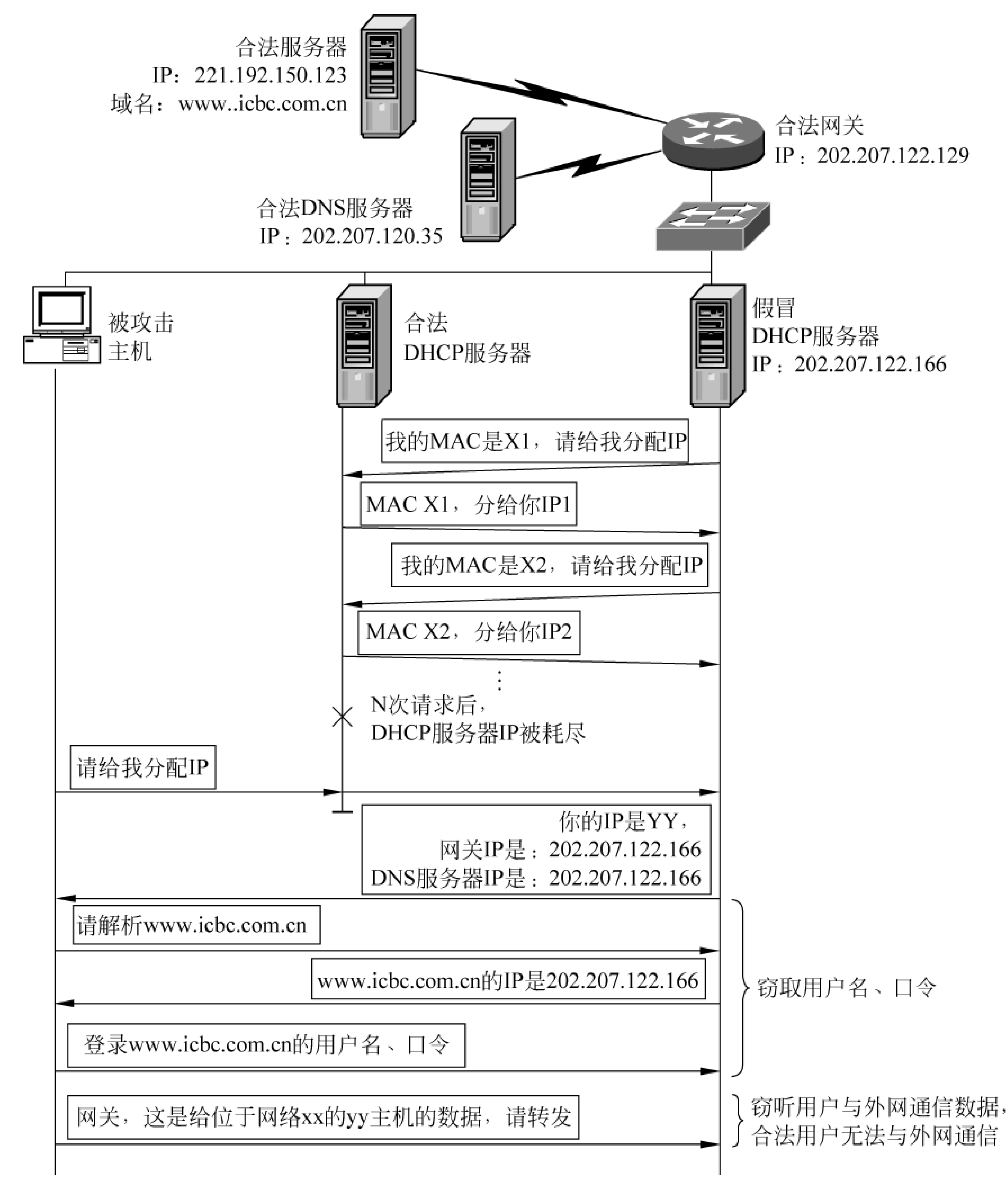


图 3-21 DHCP 攻击过程示意图

（2）对 DHCP 客户端进行的欺骗攻击

如图 3-21 所示，利用 DHCP 客户端不对 DHCP 服务器进行验证的安全漏洞，恶意用户可以对网络上发出 DHCP 请求的主机发动 DHCP 欺骗攻击。为进行 DHCP 欺骗攻击，恶意用户一般会对合法 DHCP 服务器进行 DoS 攻击，一旦网络上合法的 DHCP 服务器不能再提供服务，恶意用户就开始假冒 DHCP 服务器响应 DHCP 客户端请求，将其自身地址作为网关、DNS 服务器地址发送给希望获得 IP 地址的主机。

当被欺骗的主机开始使用假冒网关地址通信时，就会把所有到其他网络的流量发送给恶意用户主机。而如果被欺骗的主机使用获得的假 DNS 服务器地址请求解析要访问的服务器域名时，恶意用户主机又可以再假冒 DNS 服务器，将伪造的 DNS 解析结果返回给被欺骗的主机，从而将用户引导到假冒服务器上，泄露用户信息。

在交换机上配置 DHCP 监听，只从可信的端口接收 DHCP 响应报文，同时限制端口上通过的 DHCP 请求报文数，可以一定程度上防御上面所述 DHCP 攻击。

2. DHCP 监听技术

DHCP 监听（DHCP Snooping）技术主要包括以下两方面内容。

（1）定义 DHCP 可信端口

如图 3-22 所示，DHCP 监听技术通过定义哪个端口连接到可信 DHCP 服务器，来限制来自不可信端口的 DHCP 响应报文，也就可以阻止来自交换机 DHCP 不可信端口的假冒 DHCP 服务器或恶意用户发出的假冒 DHCP 响应报文。

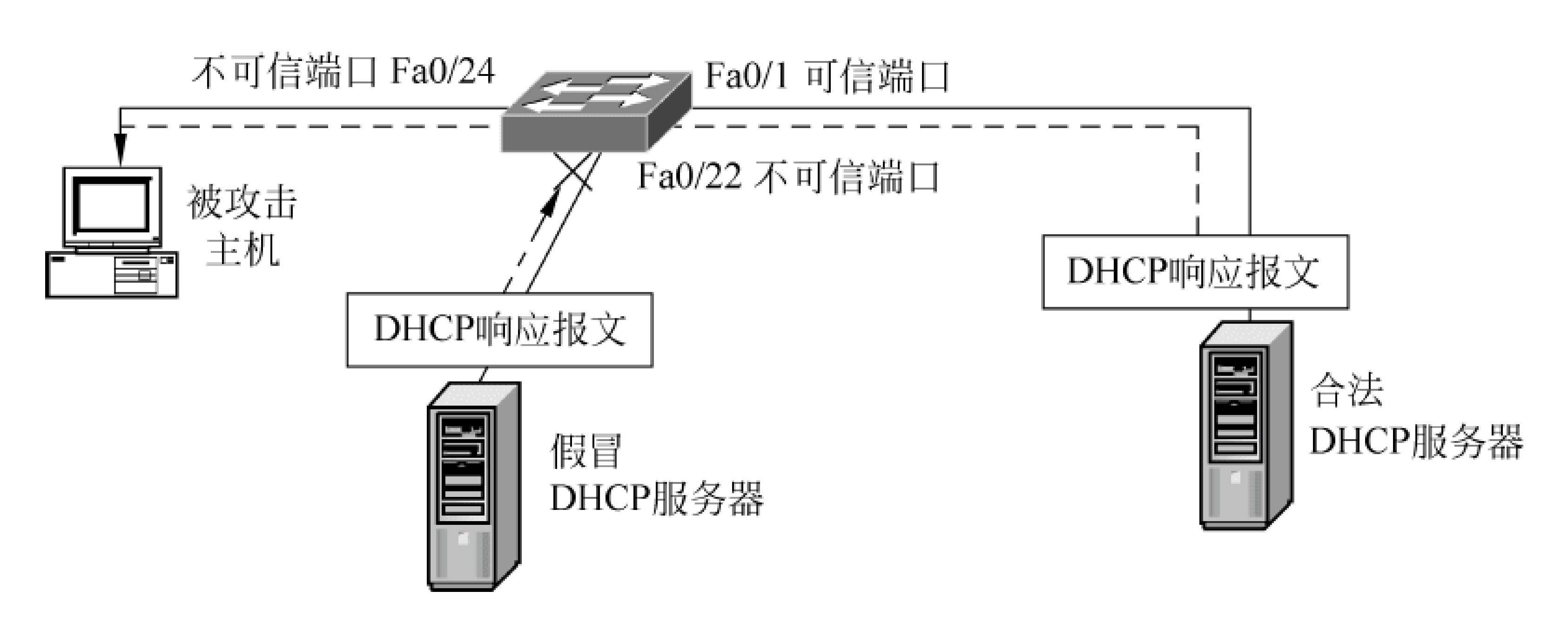


图 3-22　DHCP 监听技术可信端口工作原理示意图

（2）监听 DHCP 报文

DHCP 监听特性可以在交换机每个 VLAN 上启用。启用 DHCP 监听的交换机会拦截进入 VLAN 的所有 DHCP 流量。

对于拦截的 DHCP 响应报文，交换机主要进行两方面工作。一方面，丢弃来自非可信端口的 DHCP 响应报文，使只有连接到可信任端口的 DHCP 服务器才能分发 IP 地址；另一方面，根据来自可信端口的 DHCP 响应报文建立一个 DHCP 绑定表，内容包括客户端 IP 地址、MAC 地址、端口号、VLAN 编号、租用和绑定类型信息等，为其他安全技术，如 IP 源防护、DAI 的实施做准备。

对于拦截的 DHCP 请求报文，交换机可以根据 DHCP 请求限速配置，丢弃过量的 DHCP 请求，以保护 DHCP 服务器免受 DHCP DoS 攻击。同时如果配置使用 Option82

扩展字段，交换机还可以在 DHCP 请求报文中插入该报文入站的端口、VLAN 和交换机 MAC 等信息作为中继代理信息字段发往 DHCP 服务器，使 DHCP 服务器能够跟踪 DHCP 地址池中已分配的 IP 地址使用情况。

3.6.2 IP 地址欺骗及 IP 源防护技术简介

IP 地址欺骗攻击是指使用无效 IP 地址或者假冒他人 IP 地址发送 IP 分组欺骗接收方主机的网络攻击方法。IP 地址欺骗攻击往往是其他网络攻击手段的基础，例如前述 Smurf 攻击就是利用 IP 地址欺骗实现 DoS 攻击。

IP 源防护(IP Source Guarding，IPSG)是防御 IP 地址欺骗的技术之一，配置了 IP 源防护特性的交换机会根据配置，以 DHCP 监听获得的 DHCP 绑定表或者静态配置的 IP 源绑定信息作为 IP 源绑定条目，检查网络中数据报，如果源地址与 IP 源绑定条目能够匹配，则允许这些数据包通过，否则就将其丢弃。

为保证配置了 IPSG 的交换机在第一时间形成 IP 源绑定条目，交换机上的非可信端口，在链路开始转换为 UP 时，只允许 DHCP 数据报文通过。只有可信 DHCP 服务器分配了 IP 地址，交换机学习到 DHCP 绑定表，形成了 IP 源绑定条目后，才在端口上自动加载并计算基于端口的 PACL，允许其他流量通过。

3.6.3 ARP 攻击及 ARP 检测技术简介

目前常见的 ARP 攻击可以分为两类，即 ARP 欺骗攻击和 ARP 洪水攻击。

1. ARP 欺骗攻击及防护

ARP 欺骗攻击的基本原理如图 3-23 所示。攻击主机 PCc 假冒 PCb 向 PCa 发送多个伪造 ARP 响应报文，这些伪造 ARP 响应报文中源 IP 为 PCb 的 IP 地址，但是源 MAC 却为 PCc 的 MAC 地址。此时如果 PCb 不能正常发送 ARP 响应报文，则 PCa 会将收到的伪造 ARP 响应报文内容写入 ARP 缓存，而 PCa 发往 PCb 的通信流量，会被错误地发往 MAC 地址 aabb.ccdd.0004，即 PCc 处。

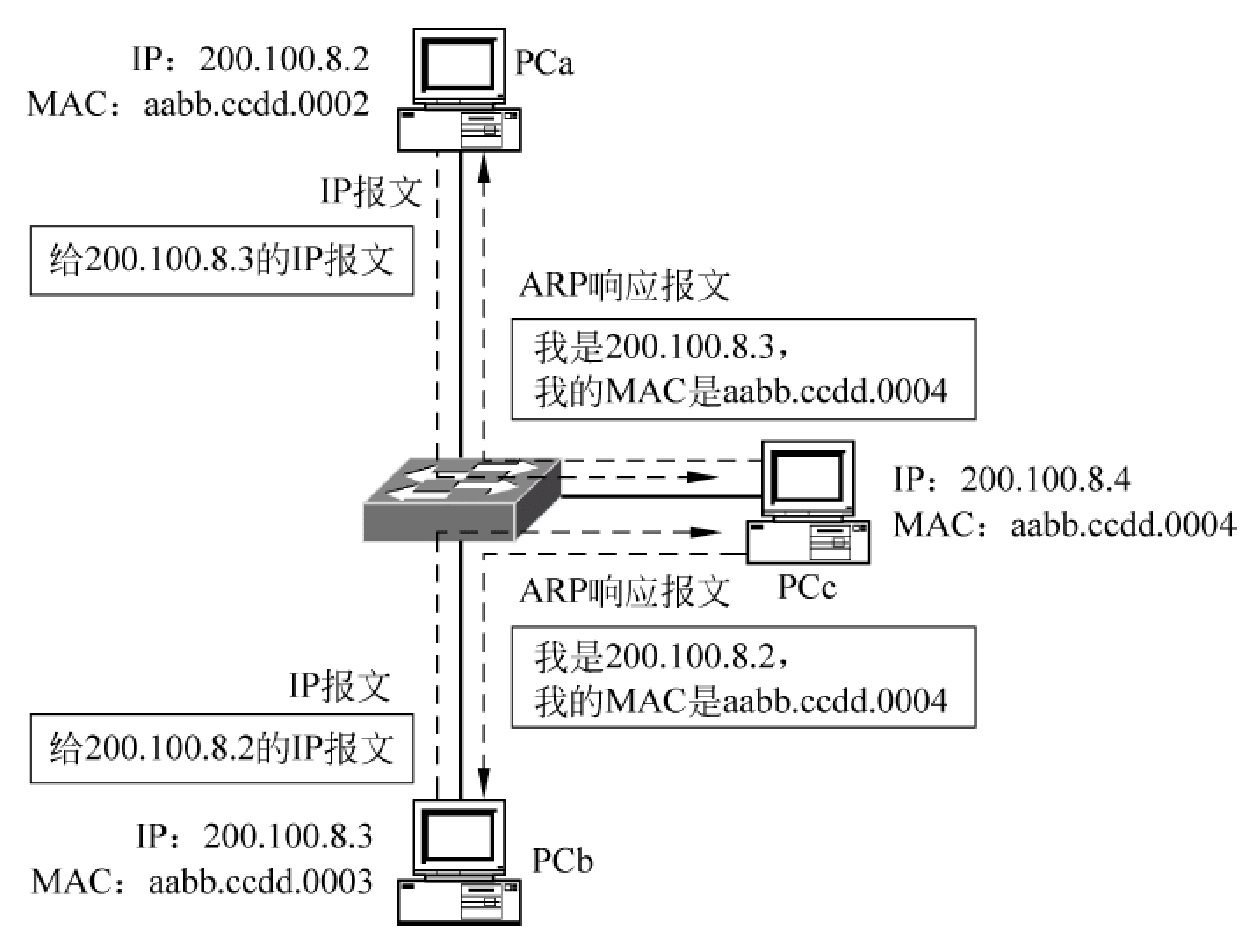


图 3-23 ARP 欺骗攻击原理示意图

一种常见的 ARP 欺骗攻击是假冒网关发送 ARP 应答报文，欺骗网络中主机将恶意主机当做网关，而把所有到外网的访问流量发送给它，这种攻击可导致被欺骗主机到其他网络的连接中断；另一种常见的 ARP 欺骗攻击是向被欺骗主机发送大量含有被欺骗主机 IP 地址的 ARP 响应报文，这种攻击可使被欺骗主机以为出现 IP 地址冲突，而被迫从网络断开，从而为恶意用户假冒被欺骗主机进行其他攻击提供方便。

要防范 ARP 欺骗攻击，可从 ARP 工作原理入手，由于静态 ARP 条目的优先级高于动态 ARP 信息，所以可以在主机和网络设备上静态绑定 ARP 条目，防范假冒 ARP 响应报文的欺骗攻击。这种防御手段有两种实施方式，一种是在主机和网络设备的 ARP 缓存中手工配置 IP 地址、MAC 地址静态绑定信息，但实施起来比较耗时，且扩展性差；另一种相对省事的做法是利用动态 ARP 检测(Dynamic ARP Inspection，DAI)结合 DHCP 监听和 IPSG 技术依据动态获得的 IP-MAC 绑定信息实施防御。

DAI 技术的基本工作原理是拦截所有进入交换机的 ARP 报文，然后将其与有效的 IP-MAC 绑定条目进行比较，匹配则通过，不匹配则丢弃。对于启用了 DHCP 监听和 DAI 的交换机，DHCP 绑定表信息将被用来作为有效 IP-MAC 绑定条目，而没有配置 DHCP 监听的交换机则以 ARP ACL 作为依据。

2. ARP 洪水攻击及防护

ARP 洪水攻击的基本原理是向网络发送大量 ARP 广播包，利用 ARP 协议短小精干且能够大量耗费交换机及网卡处理能力的特点，对交换机、路由器、主机等进行 DoS 攻击，使其因负荷过大拒绝服务，导致整个局域网掉线。进行 ARP 洪水攻击时，恶意用户可以通过修改 ARP 广播报文和数据帧中的源 MAC、源 IP 地址，防止自己在攻击时被返回流量堵塞。

目前防御 ARP 洪水攻击的方法主要是限制进入网络中的 ARP 报文流量。配置 DAI 限速可以控制进入交换机端口的 ARP 报文数量，降低 ARP 洪水攻击的力度。

3.6.4　DHCP 监听配置方法

DHCP 监听、IP 源防护与 ARP 检测技术在不同交换机上的配置操作有所不同，这些技术也不是防范 DHCP 攻击、IP 欺骗攻击、ARP 攻击的唯一方法。下面以 Cisco Catalyst 2960 交换机 12.2(50)版本的 IOS 为例介绍相应配置方法。

在 Cisco Catalyst 2960 交换机上配置 DHCP 监听的基本步骤如表 3-19 所示。

表 3-19　DHCP 监听配置步骤

序号	操　作	有关命令	是否必要
步骤 1	全局启用 DHCP 监听	**ip dhcp snooping**	是
步骤 2	指定在哪些 VLAN 上进行 DHCP 监听	**ip dhcp snooping vlan**	是
步骤 3	配置 DHCP 可信端口	**ip dhcp snooping trust**	根据网络具体情况配置
步骤 4	配置 DHCP 报文端口限速	**ip dhcp snooping limit rate**	可选
步骤 5	检查 DHCP 监听配置	**show ip dhcp snooping**	可选
步骤 6	配置是否启用 Option 选项，默认启用	**ip dhcp snooping information option**	可选

1. 启用 DHCP 监听

在 Cisco Catalyst 交换机上，启用 DHCP 监听的操作为在全局配置模式下输入：

ip dhcp snooping

在 Cisco Catalyst 交换机上，指定 DHCP 监听 VLAN 的操作为在全局配置模式下输入：

ip dhcp snooping vlan ｛VLAN 起始编号 ［ - VLAN 起始编号］｝

或者

ip dhcp snooping vlan ｛VLAN 编号 1 ［， VLAN 编号 *n* ［...］｝

例如，要在 VLAN 1 和 VLAN 10 上启用 DHCP 监听，则可以在全局配置模式下输入：

C2960(config)# **ip dhcp snooping vlan 1,10**

2. 配置 DHCP 可信端口

在 Cisco Catalyst 交换机上，启用 DHCP 可信端口的操作为在端口模式下输入：

ip dhcp snooping trust

例如，当可信 DHCP 服务器连接在交换机 Fa0/1 端口时，就可以如下配置来允许从交换机 Fa0/1 端口进入的 DHCP 响应报文。

C2960(config)# **interface fa0/1**
C2960(config-if)# **ip dhcp snooping trust**

3. 配置 DHCP 报文限速

在 Cisco Catalyst 交换机上，配置 DHCP 报文限速的操作为在端口模式下输入：

ip dhcp snooping limit rate <1-2048>

该命令最后一个参数为该端口允许的 pps，即每秒包个数，取值范围为 1～2048。

4. 检查 DHCP 监听配置

在 Cisco Catalyst 交换机上，检查 DHCP 监听配置的操作为在特权模式下输入：

show ip dhcp snooping

该命令输出结果如下。

```
C2960# show ip dhcp snooping
Switch DHCP snooping is disabled
DHCP snooping is configured on following VLANs:
1,10
DHCP snooping is operational on following VLANs:
1
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled
```

```
    circuit-id default format: vlan-mod-port
    remote-id: 0023.3478.b000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----------------        -------    -----------     ---------
FastEthernet0/1          yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/24         yes        yes             1
  Custom circuit-ids:
```

其中，显示端口 FastEthernet0/1 和 FastEthernet0/24 配置为可信端口，端口 FastEthernet0/1 没有配置限速，而端口 FastEthernet0/24 配置限速每秒仅允许 1 个报文通过。

5. 启用或禁用 Option 选项

在 Cisco Catalyst 交换机上，一旦启用 DHCP 监听，默认就会在转发的 DHCP 请求报文中插入 Option 字段信息。可以在全局配置模式下输入如下命令来禁止向 DHCP 请求报文中插入 Option 字段。

```
no ip dhcp snooping information option
```

3.6.5 IP 源防护技术配置方法

在配置 IPSG 前，需了解以下一些技术实施细节。

IPSG 只能在二层接入或干道端口配置，并且该端口不能是 DHCP 可信端口。

IPSG 对非可信端口的过滤分为基于源 IP 地址和基于源 IP 及 MAC 地址两种等级。其中，使用基于源 IP 地址过滤 IP 流量时，只有 IP 流量中的源 IP 地址与 IP 源绑定条目匹配，IP 流量才能通过交换机；使用基于源 IP 地址过滤 IP 流量时，只有 IP 流量中的源 IP 地址、MAC 地址都与 IP 源绑定条目匹配时，IP 流量才能通过交换机。

IPSG 配置分为基于 DHCP 绑定表和静态绑定两种。其中基于 DHCP 绑定表的配置步骤如表 3-20 所示，基于静态绑定的配置步骤如表 3-21 所示。

表 3-20　基于 DHCP 监听的 IPSG 配置步骤

序号	操　　作	相 关 命 令	是否必要
步骤 1	配置全局启用 DHCP 监听 指定哪些 VLAN 上进行 DHCP 监听 指定 DHCP 可信端口	ip dhcp snooping ip dhcp snooping vlan ip dhcp snooping trust	是
步骤 2	指定进行 IPSG 的端口以及过滤等级	ip verify source ip verify source port-security	根据过滤等级确定
步骤 3	检查 IPSG 源绑定条目信息 检查 DHCP 监听绑定表条目信息	show ip verify source show ip source binding debug ip verify source packet	可选

表 3-21 基于静态绑定的 IPSG 配置步骤

序 号	操 作	相 关 命 令	是否必要
步骤 1	配置静态绑定条目	ip source binding	是
步骤 2	指定进行 IPSG 的端口以及过滤等级	ip verify source ip verify source port-security	根据过滤等级确定
步骤 3	检查 IPSG 源绑定条目信息 检查 DHCP 监听绑定表条目信息	show ip verify source show ip source binding	可选

1. 指定进行 IPSG 的端口及过滤等级

在 Cisco Catalyst 2960 交换机上，指定进行 IPSG 的端口及过滤等级的操作为在端口模式下输入：

ip verify source [**port-security**]

使用该命令时，带 port-security 关键字，则表明该端口被配置为进行 IPSG，同时过滤等级为基于源 IP 和 MAC。不带 port-security 关键字，则表明该端口被配置为进行 IPSG，且过滤等级为基于源 IP。

2. 配置静态源 IP 绑定条目

在 Cisco Catalyst 2960 交换机上，静态源 IP 绑定条目的操作为在全局配置模式下输入：

ip source binding { MAC 地址 } **vlan** { VLAN 编号 } **interface** { 端口号 }

该命令定义在交换机某个端口上，只有与该命令中定义的源 IP、源 MAC 匹配的 IP 流量能够通过。

3. 检查 IPSG 配置及绑定条目信息

在 Cisco Catalyst 2960 交换机上，检查 IPSG 源绑定配置信息的操作为在特权模式下输入：

show ip verify source

该命令输出结果如下。

```
C2960#show ip verify source
Interface Filter-type  Filter-mode  IP-address        Mac-address        Vlan
-------   --------     -----      ------------------  ------------       ----
Fa0/23      ip-mac      active        200.100.8.3   F4:AA:3D:63:C7:59    1
Fa0/24      ip          active        200.100.8.5                        1
```

其中，显示端口 Fa0/23 配置使用基于源 IP、源 MAC 等级的过滤，而端口 Fa0/24 配置使用基于源 IP 等级的过滤。图中过滤模式 Filter-mode 字段，若为 active 则表明启用了 IPSG。

在 Cisco Catalyst 2960 交换机上，检查 IPSG 源绑定条目信息的操作为在特权模式下输入：

show　ip　source　binding

该命令输出结果如下。

```
C2960#show  ip  source  binding
MacAddress           IpAddress       Lease(sec)   Type          VLAN   Interface
-----------          ----------      -------      ---------     ------  -------
F4:AA:3D:63:C7:59    200.100.8.3     infinite     static           1   FastEthernet0/23
00:15:58:86:BC:EC    200.100.8.5     85414        dhcp-snooping    1   FastEthernet0/24
Total number of bindings: 2
```

其中,type 字段显示端口 Fa0/23 根据静态配置进行 IP 流量过滤,而端口 Fa0/24 配置根据 DHCP 监听获得的 IP 源绑定条目进行 IP 流量过滤。

3.6.6　DAI 配置方法

在配置 DAI 之前,还需了解以下技术实施细节。

DAI 是入站安全特性,而不是出站安全特性。即对进入交换机的 ARP 报文进行拦截处理,但不对出站 ARP 报文进行。

DAI 中可定义可信 ARP 端口,对于可信端口,交换机不进行是否匹配操作,直接转发。

DAI 依赖于 DHCP 监听产生的 IP-MAC 绑定信息对 ARP 报文进行过滤,对于没有启用 DHCP 监听的网络,则需要配置 ARP ACL 来定义允许或拒绝哪些流量。基于 DHCP 监听的 DAI 配置步骤如表 3-22 所示,基于 ARP ACL 的 DAI 配置步骤如表 3-23 所示。

表 3-22　基于 DHCP 监听的 DAI 配置步骤

序号	操　　作	有 关 命 令	是否必要
步骤 1	在 VLAN 上启用 DAI 安全特性	**ip　arp　inspection　vlan**	是
步骤 2	指定端口是否为可信 ARP 端口(交换机各端口默认为不可信端口)	**ip　arp　inspection　trust**	根据需求确定
步骤 3	检查 DAI 配置	**show　ip　arp　inspection　interfaces** **show　ip　arp　inspection　vlan**	可选
步骤 4	监测 DAI 运行	**show　ip　dhcp　snooping　binding** **show　ip　arp　inspection　statistics　vlan**	可选

表 3-23　基于 ARP ACL 的 DAI 配置步骤

序号	操　　作	有 关 命 令	是否必要
步骤 1	定义 ARP ACL	**arp　access-list** **permit**	是
步骤 2	在 VLAN 上应用 ARP ACL	**ip　arp　inspection　filter**	是
步骤 3	配置端口为非可信 ARP 端口	**no　ip　arp　inspection　trust**	是
步骤 4	在 VLAN 上打开 DAI	**ip　arp　inspection　vlan**	是
步骤 5	检查 DAI 配置	**show　arp　access-list** **show　ip　arp　inspection　vlan** **show　ip　arp　inspection　interfaces**	可选

DAI 可以在访问端口、干道端口、EtherChannel 端口和私有 VLAN 端口上配置。

1. 基于 DHCP 监听的 DAI 配置

表 3-22 显示了在 Cisco Catalyst 2960 交换机上配置基于 DHCP 监听的 DAI 基本步骤。

(1) 启用 DAI 安全特性

在 Cisco Catalyst 2960 交换机上，启用 DAI 安全特性的操作为在全局配置模式下输入：

ip arp inspection vlan { VLAN 编号 1 [{ , | - } VLAN 编号 *n* […]] }

例如，以下配置将在 VLAN 1、VLAN 10 和 VLAN20、21、…、30 上启用 DAI。

```
C2960(config)# ip arp inspection vlan 1,10,20-30
```

(2) 指定端口为可信 ARP 端口

在 Cisco Catalyst 2960 交换机上，启用 DAI 安全特性的操作为在端口配置模式下输入：

ip arp inspection trust

(3) 检查 DAI 配置

在 Cisco Catalyst 2960 交换机上，检查各端口 DAI 配置的操作为在特权配置模式下输入：

show ip arp inspection interfaces

该命令输出结果示例如下。

```
C2960# show ip arp inspection interfaces
Interface          Trust State        Rate (pps)        Burst Interval
---------          ----------         ------------      -----------
此处省略部分显示...
 Fa0/21            Untrusted              15                 1
 Fa0/22            Untrusted              15                 1
 Fa0/23            Untrusted              15                 1
 Fa0/24            Trusted               None               N/A
此处省略部分显示...
```

其中，端口 Fa0/24 由于被配置为可信 ARP 端口，因此在该端口上不进行 ARP 包过滤速率等处理。

在 Cisco Catalyst 2960 交换机上，检查各 VLAN 上 DAI 配置的操作为在特权配置模式下输入：

show ip arp inspection vlan [VLAN 编号范围]

该命令输出结果示例如下。

```
C2960# show ip arp inspection vlan 1
```

```
Source Mac Validation          : Disabled
Destination Mac Validation     : Disabled
IP Address Validation          : Disabled

 Vlan     Configuration    Operation   ACL Match     Static ACL
-----     -----------      --------    -------       -----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging       Probe Logging
-----     -----------      ------------       --------
    1     Deny             Deny               Off
```

注意：如果不指定 VLAN 编号范围参数，则默认显示所有 VLAN 的 DAI 配置信息。其中 Configuration 字段为 Enabled 表示在 VLAN 1 中已经配置了启用 DAI。

（4）监测 DAI 运行

在 Cisco Catalyst 2960 交换机上，监测各 VLAN 上 DAI 转发、丢弃 ARP 报文情况的操作为在特权配置模式下输入：

show ip arp inspection statistics vlan ［ VLAN 编号范围 ］

该命令输出结果示例如下。

```
C2960# show ip arp inspection statistics vlan 1

 Vlan     Forwarded         Dropped     DHCP Drops       ACL Drops
 ----     -------           -------     ----------       ----------
    1          4               0            0               0
 Vlan     DHCP Permits      ACL Permits   Probe Permits    Source MAC Failures
-----     ----------        -----------   ------------     -------------
    1         2                0             0                0
 Vlan   Dest MAC Failures  IP Validation Failures  Invalid Protocol Data
 ----   ---------------    ---------------         ------------------
    1          0                0                       0
```

其中显示在该 VLAN 中已经转发、丢弃的 ARP 报文数量。

2. 基于 ARP ACL 的 DAI 配置

表 3-23 显示了在 Cisco Catalyst 2960 交换机上配置基于 ARP ACL 的 DAI 基本步骤。

（1）定义 ARP ACL

在 Cisco Catalyst 2960 交换机上，定义 ARP ACL 的操作为在全局配置模式下输入：

arp access-list ｛ ARP 访问控制列表名 ｝

进入 ARP ACL 配置模式后，输入以下命令定义 IP-MAC 绑定条目：

permit ip ｛ **host** IP 地址 | **any** | 源 IP 地址 通配符 ｝ **mac** ｛ **host** MAC 地址 | **any** | 源 MAC 地址 MAC 通配符 ｝

例如，要定义 IP 为 200.100.8.2，而 MAC 为 0001.0001.0001 的 ARP ACL，则可以

输入：

```
C2960(config)# arp access-list test
C2960(config-arp-nacl)#permit ip host 200.100.8.2 mac host 1.1.1
```

(2) 应用 ARP ACL

在 Cisco Catalyst 2960 交换机上，应用 ARP ACL 的操作为在全局配置模式下输入如下命令，使用该命令可以将已经定义的 ARP ACL 应用在指定的 VLAN 中。

```
ip arp inspection filter { ARP访问控制列表名 } vlan { VLAN范围 } [ static ]
```

关键字 static 将在 ARP ACL 末尾隐含加入一条拒绝所有的语句。

(3) 检查 DAI 配置

在全局配置模式下输入如下命令，可以检查 DAI 配置情况。

```
show arp access-list [ARP访问控制列表名]
show ip arp inspection vlan { VLAN范围 }
show ip arp inspection interfaces { 接口编号 }
```

其中，show ip arp inspection interfaces 命令可以显示指定端口的 DAI 配置情况示例如下。

```
C2960#show ip arp inspection interface fa0/23
 Interface      Trust State     Rate (pps)     Burst Interval
 -----------    ------------    ------------   ---------
 Fa0/23          Untrusted          15              1
```

其中，显示端口 Fa0/23 不是 ARP 可信端口，且端口 ARP 速率限制为 15pps。

3. 限制端口 ARP 包流量的配置

表 3-24 显示了在 Cisco Catalyst 2960 交换机上配置限制端口 ARP 包流量的基本步骤。

表 3-24 限制端口 ARP 包流量配置步骤

序号	操 作	有 关 命 令	是否必要
步骤 1	配置端口 ARP 包流量	ip arp inspection limit	是
步骤 2	配置从 errdisable 状态恢复时间	errdisable recovery cause arp-inspection errdisable recovery interval	可选
步骤 3	检查端口 ARP 包流量限制 检查 errdisable 状态恢复配置	show ip arp inspection interfaces show errdisable recovery	可选

在 Cisco Catalyst 2960 交换机上，配置端口 ARP 包流量的操作为在端口配置模式下输入如下命令：

```
ip arp inspection limit { none | rate <0-2048> }
```

其中，关键字 none 表示不对端口做速率限制；关键字 rate 后可以配置端口上的 pps 大小，范围为 0～2048。

在 Cisco Catalyst 2960 交换机上，启用自动从 errdisable 状态恢复的操作为在全局配置模式下输入：

errdisable　recovery　cause　arp-inspection

在 Cisco Catalyst 2960 交换机上，配置恢复间隔的操作为在全局配置模式下输入：

errdisable　recovery　interval　{ 时间间隔 }

在 Cisco Catalyst 2960 交换机上，检查 errdisable 恢复配置的操作为在特权模式下输入：

show　errdisable　recovery

该命令输出结果示例如下。

```
C2960#show  errdisable  recovery
ErrDisable Reason              Timer Status
---------------                ----------
arp-inspection                 Enabled
此处省略部分显示...
psecure-violation              Disabled
此处省略部分显示...
Timer interval：300 seconds
Interfaces that will be enabled at the next timeout：
```

其中显示已经启用了 errdisable 恢复，且时间间隔为 300 秒。

3.6.7　模拟公司总部局域网 DHCP 监听、IP 源防护与 ARP 检测配置案例

由于 DHCP 攻击、IP 欺骗攻击和 ARP 攻击等主要侵犯当地网络，因此在模拟公司总部局域网中的接入交换机、汇聚交换机上，需要配置 DHCP 监听、IPSG 和 DAI，来保障网络通信安全。

目前模拟公司总部网络 IP 地址分配情况为：除网络中心外，其他各部门网络中的网关、服务器使用静态 IP 地址，普通主机使用动态获得的 IP 地址，DHCP 服务器连接在各楼汇聚交换机一侧。网络中心所有主机及设备均使用静态 IP。

根据以上网络实际情况和各安全特性配置限制，可实施表 3-25 所示安全配置方案。

表 3-25　各 VLAN DHCP 监听及 DAI 配置方案

<table>
<tr><th>设　备</th><th>部门
/VLAN 编号</th><th>是否启用
DHCP 监听</th><th>IP-MAC-端口-VLAN
绑定表生成方式</th><th>是否启用
DAI</th><th>ARP 绑定条目
生成方式</th></tr>
<tr><td>C2960-0-1-n</td><td>网络中心/10</td><td>不启用</td><td></td><td rowspan="6">启用</td><td>ARP ACL</td></tr>
<tr><td>C2960-0-2-n</td><td>行政管理部/20</td><td rowspan="5">启用</td><td rowspan="5">服务器为静态绑定，其他主机为 DHCP 监听</td><td rowspan="5">服务器为 ARP ACL，其他主机为 DHCP 监听</td></tr>
<tr><td rowspan="3">C2960-0-3-n</td><td>市场部/30</td></tr>
<tr><td>研发部/40</td></tr>
<tr><td>售后部/50</td></tr>
<tr><td>C2960-0-4-n</td><td>生产部/60</td></tr>
</table>

除网络中心外，其他各部门网络 VLAN 中均启用 DHCP 监听，防止假冒 DHCP 响应报文欺骗需动态获得 IP 地址的主机。

由于网络中的服务器需要使用静态 IP，所以在各接入交换机上，需要使用 ip source binding 命令为其配置 IP-MAC-端口-VLAN 绑定信息，而其他使用 DHCP 的主机使用 DHCP 监听方式自动生成绑定信息，同时对连接普通主机端口配置 IPSG。

在各网络中均启用 DAI 来防御 ARP 攻击。

除网络中心外，各部门网络 VLAN 中配置 ARP ACL 允许来自各使用静态 IP 地址服务器的流量，同时使用 DHCP 监听信息过滤来自各动态获得 IP 地址主机的流量。

各汇聚交换机下联接入交换机和上联核心交换机的端口，由于要通过多个 VLAN 的流量，因此需配置为干道端口。各汇聚交换机端口 DHCP 监听、DAI、IPSG 配置方案如表 3-26 所示。

表 3-26　各汇聚交换机端口 DHCP 监听、DAI、IPSG 配置方案

C3550-0-2-1、C3550-0-3-1、C3550-0-4-1			
	下联接入交换机的端口	连接 DHCP 服务器的端口	上联核心交换机的端口
类型	干道	接入	干道
DHCP 可信端口	不可信	可信	可信
DHCP 限速	300pps		
启用 IPSG	启用	不启用	启用
ARP 可信端口	不可信	可信	可信
ARP 限速	500pps		

由于 DHCP 服务器位于汇聚交换机一侧而不是接入交换机，因此下联各接入交换机端口需配置为不可信 DHCP 端口，另外由于 DHCP 广播不能跨越网络，因此汇聚交换机上联核心交换机的端口需配置为可信 DHCP 端口。

考虑到汇聚交换机下联网络规模(500～2000 台)、DHCP 服务工作特点(DHCP 租约期限一般较长，租约期间 DHCP 流量较少)、DHCP 服务器性能限制，因此汇聚交换机不可信 DHCP 端口 DHCP 报文速率可配置为 300pps。

在下联接入交换机的端口配置 IPSG，可以防范来自各部门网络内的 IP 欺骗攻击。

将下联接入交换机的端口配置为不可信 ARP 端口，可以防御跨交换机 VLAN 内的 ARP 攻击。由于 ARP 攻击局限在一个网络内部，因此连接 DHCP 服务器、核心交换机的汇聚交换机端口可配置为可信 ARP 端口。

考虑到汇聚交换机下联网络规模(500～2000 台)、ARP 协议工作特点、DHCP 服务器性能限制，因此汇聚交换机不可信 DHCP 端口 ARP 报文速率可配置为 500pps。

接入交换机因为要通过上联端口传输多个 VLAN 流量，所以上联端口配置为干道模式，下联主机为安全起见，一律配置为接入模式。各接入交换机端口 DHCP 监听、DAI、IPSG 配置方案如表 3-27 所示。

表 3-27　各接入交换机端口 DHCP 监听、DAI、IPSG 配置方案

C2960-0-2-*n*、C2960-0-3-*n*、C2960-0-4-*n*		
	下联主机端口	上联汇聚交换机的端口
类型	接入	干道
DHCP 可信端口	不可信	可信
DHCP 限速	15pps	
启用 IPSG	启用	不启用
ARP 可信端口	不可信	可信
ARP 限速	50pps	

恶意用户或感染了病毒或木马的主机可能通过接入端口使用 DHCP 欺骗等攻击网络内其他主机，因此连接各主机的端口配置为 DHCP 不可信端口。

连接单台主机的端口，正常发送的 DHCP 报文数量有限，因此限速为 15pps。

如上所述，连接恶意用户可能会在交换机接入端口发动 IP 欺骗攻击，所以需配置 IPSG。

恶意用户或感染了病毒或木马的主机可能通过接入端口使用 ARP 欺骗等攻击网络内其他主机，因此连接各主机的端口配置为 ARP 不可信端口。

连接单台主机的端口，正常发送的 ARP 报文数量有限，建议限速为 50pps。

3.7　私有 VLAN

3.7.1　私有 VLAN 与受保护端口技术简介

使用 ACL 可以限制网络中各主机之间的访问，但需要在每个端口配置管理 ACL，增加了管理复杂度。私有 VLAN(Private VLAN，PVLAN)和受保护端口技术可以在二层将交换机上的端口完全隔离开来，阻塞 VLAN 内主机间的通信，防御 VLAN 内主机间的彼此攻击。

受保护端口与 PVLAN 区别在于，受保护端口技术只能在本地交换机上隔离各端口，而 PVLAN 不但能在本地实现端口间的隔离，还可以在多个交换机上实现。

私有 VLAN 支持以下 3 类通信端口，实现端口间通信隔离。

(1) 混杂(Promiscuous)端口。能够与所有端口通信，包括 PVLAN 中的隔离、团体端口。该种端口一般用于连接上级网络设备。

(2) 孤立(Isolated)端口。只能与同一个 PVLAN 中的混杂端口通信。孤立 VLAN 从二层上完全与同一个 PVLAN 中除混杂端口外的其他端口隔离开来。

(3) 团体(Community)端口。能与同一个 PVLAN 中同一团体内的其他端口通信，也能与同一个 PVLAN 中的混杂端口通信，但从二层上完全与同一个 PVLAN 中的其他团体内的端口或者孤立端口隔离开来。

对应于以上 3 种端口类型，PVLAN 结构中存在以下 3 种 PVLAN。

(1) 主 VLAN(Primary VLAN)。混杂端口位于主 VLAN 中。主 VLAN 可以把位于其中的混杂端口的流量传送到孤立 VLAN、团体 VLAN，以及同一个主 VLAN 中的其他混杂端口。

（2）孤立 VLAN。孤立端口位于孤立 VLAN 中，孤立 VLAN 将其中孤立端口的流量传送到一个混杂端口。

（3）团体 VLAN。团体端口位于团体 VLAN 中，团体 VLAN 将位于其中的团体端口的流量传送到同一团体 VLAN 内的团体端口，也可以传送到混杂端口，但不能传送到其他团体 VLAN。

注意：孤立 VLAN、团体 VLAN 也叫次 VLAN(Secondary VLAN)。在一个私有 VLAN 中，可以有一个主 VLAN 和多个次 VLAN。可以通过 PVLAN Trunk 端口在多个交换机上扩展 PVLAN。

3.7.2 受保护端口、私有 VLAN 配置方法

1. 受保护端口配置

大部分 Cisco Catalyst 交换机都支持受保护端口功能。

在 Cisco Catalyst 交换机上，配置受保护端口的操作为在端口配置模式下输入：

switchport protected

在 Cisco Catalyst 交换机上，检查端口是否已被配置为受保护端口的操作为在特权模式下输入：

show interface 端口号 **switchport**

2. 私有 VLAN 配置

配置 PVLAN 的步骤如表 3-28 所示。配置 PVLAN 的基本步骤可以简单理解为首先搭建一个主 VLAN、若干孤立 VLAN 和团体 VLAN，并将次 VLAN 关联到主 VLAN，然后配置端口模式为混杂、孤立、团体端口，并将端口映射到主 VLAN、关联到次 VLAN。

表 3-28 PVLAN 配置基本步骤

序号	操 作	有 关 命 令	必要性
步骤 1	配置交换机 VTP 模式为透明模式	**vtp mode transparent**	是
步骤 2	配置 VLAN 为 PVLAN，并设置 PVLAN 类型	**private-vlan**	是
步骤 3	将次 VLAN 关联到主 VLAN	**private-vlan association**	是
步骤 4	配置一个混杂端口，并将该混杂端口加入到主 VLAN 中	**switchport mode private-vlan promiscuous** **switchport private-vlan mapping**	是
步骤 5	配置端口为孤立端口或团体端口，映射主 VLAN、关联次 VLAN	**switchport mode private-vlan host** **switchport private-vlan mapping**	是
步骤 6	检查 PVLAN 配置 检查端口 PVLAN 配置	**show vlan private-vlan** **show interface**	可选

注意：PVLAN 并不是在所有 Cisco Catalyst 交换机上都能得到支持。

下面以 C4500 系列交换机的 PVLAN 配置为例。

（1）配置 VLAN 为 PVLAN。在 Cisco Catalyst 交换机上，配置 VLAN 为 PVLAN

的操作为在 VLAN 配置模式下输入：

private-vlan { **isolated** | **primary** | **community** }

使用关键字 isolated 意为将 PVLAN 配置为孤立 VLAN，使用关键字 primary 意为将 PVLAN 配置为主 VLAN，使用关键字 community 意为将 PVLAN 配置为团体 VLAN。

例如，将 VLAN20 配置为主 VLAN。

```
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan  primary
Switch(config-vlan)# end
```

注意：只有退出 VLAN 配置模式时，该命令才会真正生效。

(2) 将次 VLAN 关联到主 VLAN。在 Cisco Catalyst 交换机上，将次 VLAN 关联到主 VLAN 的操作为在主 VLAN 配置模式下输入：

private-vlan association { 次 VLAN 编号 | **add** 次 VLAN 编号 | **remove** 次 VLAN 编号 }

其中，使用 add 关键字并且跟随一个次 VLAN 编号的作用与直接输入次 VLAN 编号的作用相同，都用于将一个次 VLAN 与主 VLAN 关联起来。而使用 remove 关键字，并且跟随一个次 VLAN 编号，则会删除该次 VLAN 与主 VLAN 的关联关系。

(3) 配置一个混杂端口，并将其映射到主 VLAN。在 Cisco Catalyst 交换机上，配置一个端口模式为混杂模式的操作为在端口配置模式下输入：

switchport mode private-vlan promiscuous

在 Cisco Catalyst 交换机上，将混杂端口映射到主 VLAN 的操作为在端口配置模式下输入：

switchport private-vlan mapping [**trunk**] 主 VLAN 编号 { 次 VLAN 编号 | **add** 次 VLAN 编号 | **remove** 次 VLAN 编号 }

该命令将混杂端口映射到主 VLAN，以及相关联的次 VLAN。

例如，下面命令将端口 Fa0/2 配置为混杂端口，然后映射到主 VLAN20，关联到次 VLAN21。

```
Switch(config)# interface  fastethernet 0/2
Switch(config-if)# switchport  mode  private-vlan  promiscuous
Switch(config-if)# switchport  private-vlan  mapping  200  210
Switch(config-if)# end
```

(4) 配置端口为孤立端口或团体端口，映射到主 VLAN、关联次 VLAN。在 Cisco Catalyst 交换机上，将端口配置为 host 端口(孤立端口或团体端口)的操作为在端口配置模式下输入：

switchport mode private-vlan host

在 Cisco Catalyst 交换机上，将端口映射到主 VLAN、关联次 VLAN 的操作参见前面配置。

（5）检查 PVLAN 和端口 PVLAN 配置。在 Cisco Catalyst 交换机上，检查 PVLAN 的操作为在特权模式下输入：

show vlan private-vlan

该命令输出结果如下。注意，其中团体 VLAN 318 没有正确关联到主 VLAN。

```
Primary  Secondary   Type          Interfaces
------   ---------   -----------   ------------
300      301         community
300      302         community
300      303         community
300      311         isolated
318                  community
```

在 Cisco Catalyst 交换机上，检查端口 PVLAN 的操作为在特权模式下输入：

show interfaces 端口号 switchport

该命令输出结果如下。

```
Name:Fa0/2
Switchport:Enabled
Administrative Mode:private-vlan promiscuous                                                  ①
Operational Mode:private-vlan promiscuous                                                     ②
此处省略部分显示...
Negotiation of Trunking:Off
此处省略部分显示...
Administrative Private VLAN Host Association:none                                             ③
Administrative Private VLAN Promiscuous Mapping:300 (VLAN0300) 302 (VLAN0302)                 ④
Private VLAN Trunk Native VLAN:none
Administrative Private VLAN Trunk Encapsulation:dot1q
Administrative Private VLAN Trunk Normal VLANs:none
Administrative Private VLAN Trunk Private VLANs:none
Operational Private VLANs:                                                                    ⑤
300 (VLAN0300) 302 (VLAN0302)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001                                                                  ⑥
此处省略部分显示...
```

其中：

① 该端口模式被配置为混杂端口。

② 该端口模式目前状态是混杂端口。

③ none 表示该端口没有被配置为 Host 端口。

④ 该端口被配置映射到主 VLAN300，关联到次 VLAN302。

⑤ 该端口目前工作的 PVLAN 有主 VLAN300 和次 VLAN302。

⑥ PVLAN 只能被配置到 VLAN2～VLAN1001 上。

3.7.3　模拟公司总部局域网 PVLAN 配置

根据 3.5.3 小节所述，为实现模拟公司市场部主机间不能互访的安全需求，在不更换接入交换机的情况下，可以在该部门网络连接的接入交换机 C2960-0-3-*n* 上配置受保护端口。但如果可以使用 Cisco 4500 系列交换机替换现有 C2960 接入交换机，则可以在该接入交换机上配置 PVLAN，来隔离主机间通信。

3.8　VLAN 跳跃攻击与防护

由于 Cisco Catalyst 交换机各端口的干道选择模式默认为 auto，所以如果交换机在加入到网络中时，没有修改端口干道选择模式，就非常容易受到 VLAN 跳跃攻击。图 3-24 显示了一种 VLAN 跳跃攻击方式。

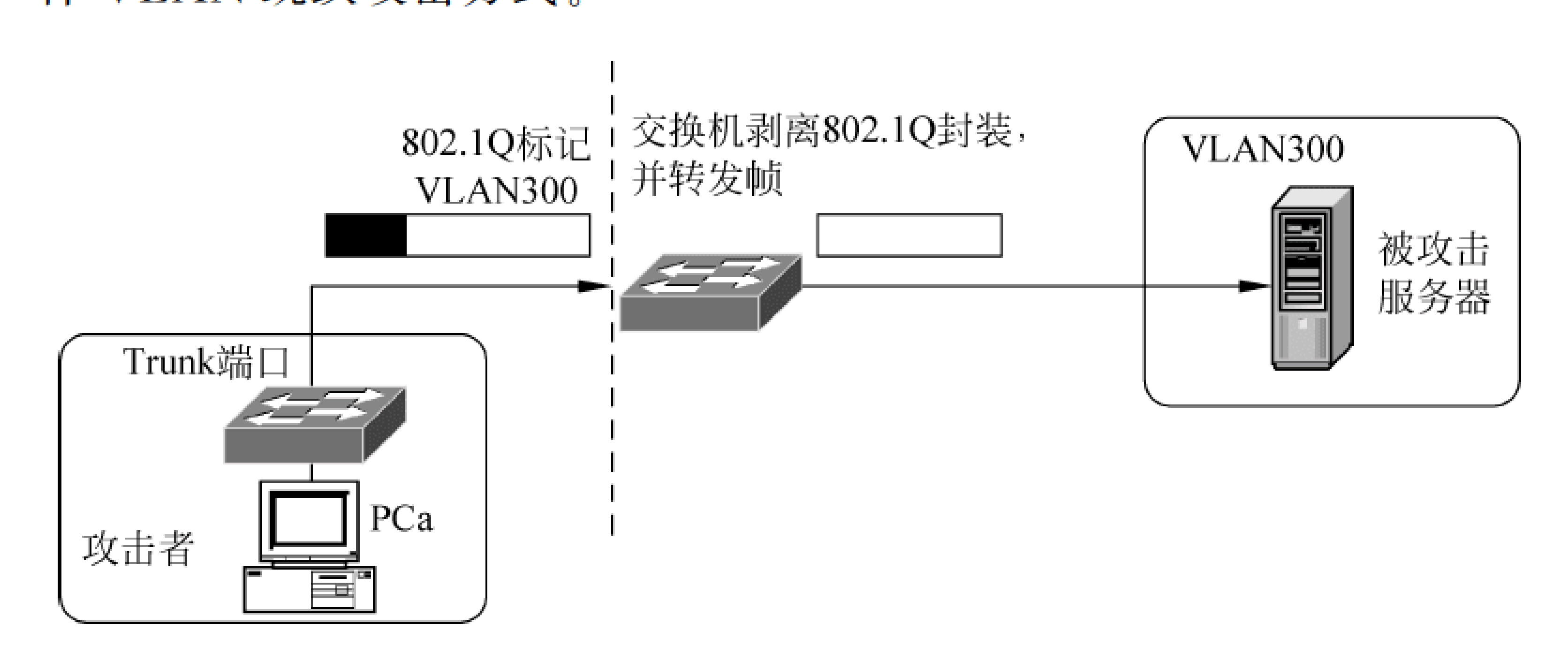


图 3-24　VLAN 跳跃攻击示例

图 3-24 中，攻击者将攻击用交换机的 Trunk 端口连接到网络中的交换机。这样，网络中的交换机端口模式就转变为干道模式，攻击者就可以访问干道连接的各 VLAN 中主机。

要防护这种 VLAN 跳跃攻击非常简单，只需要注意修改接入网络中的交换机端口干道选择模式，对于非必要干道端口，应均配置为接入模式。

3.9　小结

局域网安全常用网络安全技术有：端口安全技术、IEEE 802.1.x、交换机访问控制、DHCP 监听、IP 源防护、动态 ARP 检测、私有 VLAN。端口安全可以将端口与特定 MAC 绑定起来，保证从端口入站数据帧是可靠的。IEEE 802.1x 提供了局域网主机通过 EAP 消息传递身份认证信息的方式。交换机支持 RACL、VACL、PACL 等多种访问控制。DHCP 监听、IP 源防护和动态 ARP 检测技术可以保护交换机抵抗 DHCP 欺骗、IP 欺骗和 ARP 攻击。私有 VLAN 技术提供了在更细颗粒度的 VLAN 技术。

3.10 习题

1. 下列哪条命令可以在 Cisco IOS 的交换机上启用 AAA？（　　）

A. aaa　authentication　　B. aaa　new-model

C. radius-server　host　　D. login　authentication

2. RADIUS 协议使用哪种传输层协议？（　　）

A. TCP　　B. UDP　　C. FTP　　D. HTTP

3. RADIUS 客户端与服务器使用什么进行验证？（　　）

A. 一次性口令（OTP）　　B. 共享密钥

C. 令牌　　D. 非对称密钥

4. 在管理员成功通过身份验证后，（　　）功能用于允许其访问网络中的资源。

A. 访问控制　　B. 身份验证　　C. 授权　　D. 记账

5. 管理员发现在网络中进行 AAA 配置后不能远程登录到网络设备上进行管理，此时应使用什么命令进行排错？（　　）

A. show　accounting

B. debug　aaa　accounting

C. debug　radius　accounting

D. debug　aaa　authentication

E. debug　radius　authentication

F. show　login

6. IEEE 802.1x 体系结构中定义了哪 3 类角色？（　　）

A. 请求者　　B. 授权者　　C. 认证者　　D. 认证服务器

E. 客户端

7. 请求者与授权者间将 EAP 消息封装在哪个数据结构中？（　　）

A. 数据帧　　B. UDP 报文　　C. TCP 报文　　D. ARP 报文

8. 下列哪种 ACL 可以应用到二层端口上？（　　）

A. RACL　　B. PACL　　C. VACL　　D. 以上全是

9. 交换机的哪种安全特性可以用来防御 MAC 欺骗攻击？（　　）

A. IPSG　　B. DAI　　C. DHCP 监听　　D. 端口安全

10. 防范 MAC 泛洪攻击可以通过配置哪项安全配置实现？

A. IPSG　　B. DAI　　C. DHCP 监听　　D. 端口安全

E. PACL

11. 判断题：交换机端口安全配置 sticky 选项可以降低端口安全配置工作。

12. 判断题：交换机端口安全配置使用静态绑定 MAC 在交换机端口重启后会失效。

13. 交换机的哪种特性可以防御 ARP 攻击？（　　）

A. IPSG　　B. DAI　　C. DHCP 监听　　D. 端口安全

14. 检查 DHCP 监听获得的 DHCP 绑定表的命令是(　　)。

A. show ip source binding　　B. show ip dhcp snooping binding

C. show ip arp inspection vlan　　D. show ip dhcp snooping

15. 使用哪条命令可以检查 IPSG 绑定条目？(　　)

A. show ip source binding　　B. show ip dhcp snooping binding

C. show ip arp inspection vlan　　D. show ip dhcp snooping

16. 使用哪条命令可以检查 DAI 是否已经配置在端口上？(　　)

A. show ip source binding　　B. show ip dhcp snooping binding

C. show ip arp inspection vlan　　D. show ip arp inspection interface

17. IPSG 绑定条目信息包括哪些内容？(　　)

A. MAC 地址、IP 地址、租期、绑定类型、DHCP 地址池名、VLAN 编号、该条目对应的不可信交换机端口号

B. MAC 地址、IP 地址、租期、绑定类型、DHCP 地址池名、VLAN 编号、该条目对应的可信交换机端口号

C. MAC 地址、租期、绑定类型、DHCP 地址池名、VLAN 编号、该条目对应的不可信交换机端口

D. MAC 地址、IP 地址、租期、DHCP 地址池名、VLAN 编号、该条目对应的不可信交换机端口

18. 判断题：DHCP 绑定表与 IPSG 绑定条目内容完全相同。

19. 私有 VLAN 结构中定义了哪些类型的 PVLAN？(　　)

A. isolated　　B. primary　　C. community　　D. promiscuous

E. secondary

20. 哪种方法是防御 VLAN 跳跃攻击的必要手段？(　　)

A. 关闭端口的干道协商

B. 配置端口工作在全双工

C. 配置端口工作在干道选择的 auto 模式

D. 配置启用端口安全

3.11　实训

3.11.1　AAA 配置

1. 实训组织

实训学时：50 分钟。

学生分组：2 人/组。

2. 实训目的

通过实训熟练掌握：RADIUS 服务器安装、配置；网络设备上 AAA 身份验证、授权、记账配置的基本方法和操作。

3. 实训环境

(1) 安装有 Windows 系统并保存有 FreeRADIUS.net 安装软件的 PC,每组 2 台。

(2) Cisco 二层交换机,每组 1 台。

(3) Cisco 三层交换机或路由器,每组 1 台。

(4) UTP 直通电缆,每组 2 条。

(5) UTP 交叉电缆,每组 1 条。

(6) Console 电缆,每组 2 条。

注意:保持所有的交换机、路由器为出厂配置。Cisco 网络设备的 IOS 要支持 SSH 功能。

4. 实训准备

本实训网络拓扑如图 3-25 所示,该图对图 3-1 模拟公司总部局域网拓扑示意图进行了适当简化。图中各网络设备、RADIUS 服务器、PC VLAN 及 IP 地址配置如表 3-29 所示。

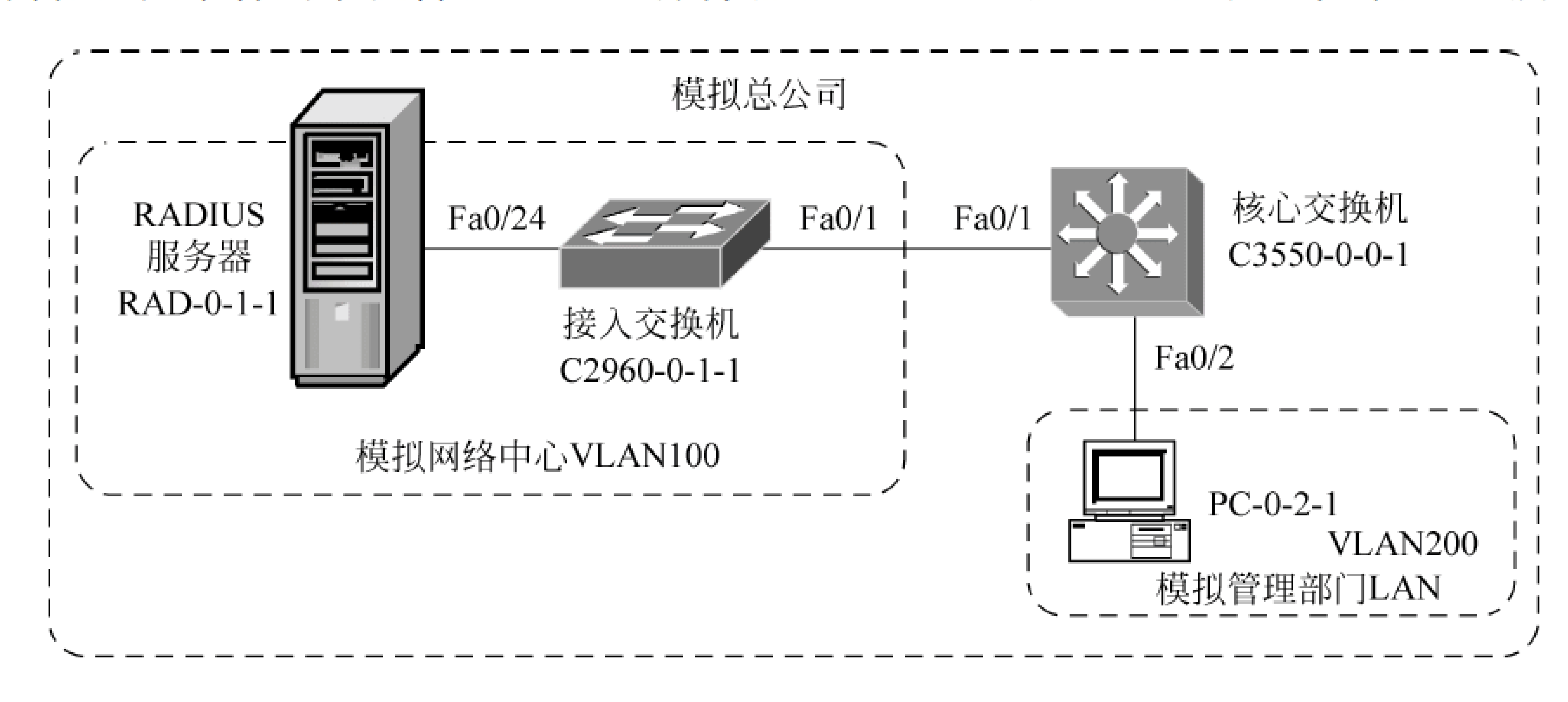


图 3-25 AAA 实训网络拓扑示意图

图 3-25 中核心交换机 C3550-0-0-1 模拟公司总部局域网的核心交换机,该交换机实现模拟网络中管理部门 LAN 和网络中心 LAN 间数据的路由。PC-0-2-1 模拟管理部门 LAN 内的计算机,本实训中要模拟网络管理员从该计算机使用 Telnet/SSH 远程登录核心交换机 C3550-0-0-1 和接入交换机 C2960-0-1-1 的 AAA 身份验证、记账配置。

实训前需按图 3-25 所示拓扑搭建实训所需网络,并按照表 3-29 完成网络连通性配置。有关管理 VLAN、VLAN 间路由等有关内容可参见本系列教材中《计算机网络集成技术》、《计算机网络技术基础》等。

注意:

(1) 在核心交换机 C3550-0-0-1 上需创建 VLAN99、VLAN11 和 VLAN12。其中 VLAN99 作为该交换机的管理 VLAN,VLAN11 为网络中心所在 VLAN,VLAN12 为管理部门所在 VLAN。本实训环境中通过配置核心交换机 C3550-0-0-1 的 VLAN 虚接口,实现 VLAN 间路由。各 VLAN 虚接口 IP 如表 3-29 所示。

(2) 在接入交换机 C2960-0-1-1 上需创建 VLAN11 和 VLAN99,其中 VLAN99 用于管理 VLAN,VLAN11 为网络中心所在 VLAN。接入交换机 C2960-0-1-1 的管理 VLAN

虚接口 IP 如表 3-29 所示，注意要为该交换机配置默认网关，以保证其他网络的主机能访问该网络设备。

表 3-29　AAA 实训网络设备 VLAN、IP 地址分配

设备名称	VLAN ID	VLAN name	VLAN 虚接口 IP 地址/网络前缀	SSH 所属域
C3550-0-0-1	管理 VLAN：99 VLAN：10 VLAN：200	mgmt nic admin	VLAN99：200.100.8.65/26 VLAN10：200.100.8.1/26 VLAN200：200.100.8.129/25	sjzpc.edu.cn
C2960-0-1-1	管理 VLAN：99 VLAN：100	mgmt nic	VLAN99：200.100.8.66/26	sjzpc.edu.cn

（3）RADIUS 服务器和测试 PC 的 IP 配置如表 3-30 所示。

表 3-30　AAA 实训主机 VLAN、IP 地址分配

主 机 名 称	所属 VLAN	IP 地址/网络前缀	网关 IP
RAD-0-1-1	VLAN：10	200.100.8.30/26	200.100.8.1
PC-0-2-1	VLAN：20	200.100.8.254/25	200.100.8.129

5. 实训内容

（1）模拟公司总部局域网 RADIUS 服务器安装、配置。

要求：安装配置一台 RADIUS 服务器，客户端与其共享密钥为 Net&Sec@sjzpc；网络设备远程登录用户名为自己姓名拼音，口令为自己学号，例如用户名为 th，口令为 01。

（2）模拟公司总部局域网网络设备 AAA 身份验证、记账配置。

要求：配置对 Telnet 到 C2960-0-1-1 和 SSH 到 C3550-0-0-1 进行身份验证；对登录后 exec、connection 事件进行记账。

（3）AAA 配置验证。

要求：测试能否使用配置的用户名、口令登录 C3550-0-0-1、C2960-0-1-1；测试如果输入用户名、口令错误，RADIUS 服务器不工作时能否登录网络设备，思考一旦出现以上问题的备用方案；使用 debug aaa authentication、debug aaa accounting、debug radius authentication、debug radius accounting 命令观察 AAA 工作过程。

（4）记账记录分析。

要求：分析 FreeRADIUS.net 身份验证和记账记录，对照 AAA 配置，检查是否进行了正确的记账；分析连续多次错误输入用户名、口令情况下，记账记录有什么特点。

6. 实训指导

（1）检查网络连通性。

启动进入 PC-0-2-1 系统，在 CMD 窗口输入 ping　200.100.8.65、ping　200.100.8.66、ping　200.100.8.30 命令分别测试到达 C3550-0-0-1、C2960-0-1-1 管理 VLAN 虚接口以及 RAD-0-1-1 的网络连通性，应均能 ping 通。

使用 console 方式连接到 C3550-0-0-1、C2960-0-1-1，使用 show 命令检查网络连通性

配置，填写实训报告。

（2）RADIUS 服务器安装、配置。

参考 3.2.2 小节，在 RAD-0-1-1 上安装、配置 FreeRADIUS.net。

修改 clients.conf 文件，在文件其他 clients 定义内容末增加如下内容。

```
client   200.100.8.65/26 {
secret         =   Net&Sec@sjzpc
shortname      =   C3550-0-0-1
}
client   200.100.8.66/26 {
secret         =   Net&Sec@sjzpc
shortname      =   C2960-0-1-1
}
```

修改 users.conf 文件，在该文件其他用户定义内容末增加如下内容。

```
用户名      User-Password == "用户密码"
```

配置完成后，启动 FreeRADIUS.net 服务。

（3）配置 C3550-0-0-1 启用 SSH。

使用 console 方式连接 C3550-0-0-1，打开超级终端窗口，进入全局配置模式，输入如下命令。

```
Switch(config)#hostname   C3550-0-0-1                                        ①
C3550-0-0-1(config)#ip   domain-name   sjzpc.edu.cn                          ②
C3550-0-0-1(config)#crypto   key   generate   rsa                            ③
The name for the keys will be: C3550-0-0-1.sjzpc.edu.cn                      ④
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048                                     ⑤
% Generating 2048 bit RSA keys ...[OK]

C3550-0-0-1(config)#
*Mar  1 00:02:59.407: %SSH-5-ENABLED: SSH 1.5 has been enabled               ⑥
```

其中：

① 配置核心交换机 C3550-0-0-1 的主机名，为创建 SSH 密钥做准备。

② 配置核心交换机 C3550-0-0-1 的域名，为创建 SSH 密钥对做准备。

③ 使用 crypto key generate rsa 命令为核心交换机创建 SSH 密钥对。

④ 开始创建密钥对，程序提示密钥对的名字为 C3550-0-0-1.sjzpc.edu.cn。

⑤ 创建密钥对程序提示输入密钥长度，此处选择 2048。

⑥ 创建密钥对成功，创建密钥对程序提示已经可以着手配置 SSH 功能。

（4）配置 C3550-0-0-1 使用 RADIUS 进行 AAA 身份验证、记账。

在全局配置模式，输入如下命令。

```
C3550-0-0-1(config)#aaa   new-model
```

```
C3550-0-0-1(config)#radius-server host 200.100.8.30 auth-port 1812 acct-port 1813
C3550-0-0-1(config)#radius-server key Net&Sec@sjzpc
C3550-0-0-1(config)#aaa authentication login ssh-auth-in group radius line
C3550-0-0-1(config)#aaa accounting connection ssh-acc-conn group radius
C3550-0-0-1(config)#aaa accounting exec ssh-acc-exec start-stop group radius
C3550-0-0-1(config)#line vty 0 4
C3550-0-0-1(config-line)#login authentication ssh-auth-in
C3550-0-0-1(config-line)#accounting connection ssh-acc-conn
C3550-0-0-1(config-line)#accounting exec ssh-acc-exec
C3550-0-0-1(config-4line)#transport input ssh
```

(5) 配置 C2960-0-1-1 使用 RADIUS 进行 AAA 身份验证、记账。

使用 console 方式连接 C2960-0-1-1，打开超级终端窗口，进入全局配置模式，输入如下命令。

```
C2960-0-1-1(config)#aaa new-model
C2960-0-1-1(config)#radius-server host 200.100.8.30 auth-port 1812 acct-port 1813
C2960-0-1-1(config)#radius-server key Net&Sec@sjzpc
C2960-0-1-1(config)#aaa authentication login tel-auth-in group radius
C2960-0-1-1(config)#aaa accounting connection tel-acc-conn start-stop group radius
C2960-0-1-1(config)#aaa accounting exec tel-acc-exec start-stop group radius
C2960-0-1-1(config)#line vty 0 4
C2960-0-1-1(config-line)#login authentication tel-auth-in
C2960-0-1-1(config-line)#accounting connection tel-acc-conn
C2960-0-1-1(config-line)#accounting exec tel-acc-exec
```

(6) 打开调试信息，测试 AAA 配置。

分别在 C3550-0-0-1、C2960-0-1-1 上，进入特权配置模式，输入如下命令，显示网络设备 aaa 和 radius 调试信息。

```
C2960-0-1-1#debug aaa authentication
AAA Authentication debugging is on
C2960-01-1#debug aaa accounting
AAA Accounting debugging is on
C2960-0-1-1#debug radius authentication
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol (authentication) debugging is on
Radius packet protocol (accounting) debugging is off
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging is off
C2960-0-1-1#debug radius accounting
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
```

```
Radius packet protocol debugging is on
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging is off
```

在 PC-0-2-1 上 CMD 窗口中，分别运行 Telnet 200.100.8.65、Telnet 200.100.8.66，出现登录窗口时，输入正确的用户名、口令，测试能否登录。同时观察网络设备上的调试输出信息。

再从 PC-0-2-1 上多次登录 C3550-0-0-1、C2960-0-1-1，输入任意用户名、口令，观察调试信息输出。

将 C2960-0-1-1 的 Fa0/24 端口宕掉，再从 PC-0-2-1 上登录 C3550-0-0-1、C2960-0-1-1，输入正确的用户名、口令，观察调试信息输出。

（7）检查记账信息。

在 RAD-0-1-1 上打开 FreeRADIUS.net 记账记录所在目录，查看记账信息。应能在 FreeRADIUS.net 安装目录下的 var\log\radius\radacct\子目录中找到目录名为 200.100.8.65 和 200.100.8.66 的子目录，打开子目录应能看到 auth-detail-日期.log、detail-日期.log、reply-detail-日期.log 等文件。使用文本编辑器打开这些文件，检查其中的记账信息，看是否符合配置要求。

7. 实训报告

网络连通性检查	设　　备	接　　口	IP 地址/网络前缀/默认网关
	C3550-0-0-1	interface Vlan99	
		interface Vlan10	
		interface Vlan200	
	C2960-0-1-1	interface Vlan99	
	RAD-0-1-1		
	PC-0-2-1		
	测试连通性命令	测试结果	原因分析
	ping 200.100.8.65		
	ping 200.100.8.66		
FreeRADIUS 服务器配置	配置文件	配置项目	配置指令
	clients.conf 文件	有关 200.100.8.65 客户端的配置	
		有关 200.100.8.66 客户端的配置	
	users.conf 文件	用户名、口令配置	
C3550-0-0-1 AAA 配置	配置项	配 置 命 令	
	创建密钥对启用 SSH		
	启用 AAA		
	RADIUS 服务器信息		
	身份验证		
	记账		

续表

C2960-0-1-1 AAA 配置	启用 AAA			
	RADIUS 服务器			
	信息			
	身份验证			
	记账			
C3550-0-0-1AAA 配置调试	远程登录序号	用户名/口令	调试输出的关键信息	
	第 1 次（正确用户名/口令）		aaa authentication	
			aaa accounting	
			radius authentication	
			radius accounting	
	第 2 次（错误用户名/口令）		aaa authentication	
			aaa accounting	
			radius authentication	
			radius accounting	
	第 3 次 RADIUS 服务器掉线		aaa authentication	
			aaa accounting	
			radius authentication	
			radius accounting	
C2960-0-1-1AAA 配置调试	第 1 次（正确用户名/口令）		aaa authentication	
			aaa accounting	
			radius authentication	
			radius accounting	
RADIUS 记账信息分析	事件	记账记录关键信息		
	第 1 次登录 C3550-0-0-1	登录记录 退出登录记录		
	第 2 次登录 C3550-0-0-1	登录记录 退出登录记录		
	第 3 次登录 C3550-0-0-1	登录记录 退出登录记录		
	第 1 次登录 C2960-0-0-1 后再远程登录 C3550-0-0-1	登录记录 退出登录记录 对外 Telnet 连接记录		

3.11.2　交换机端口安全配置

1. 实训组织

实训学时：100 分钟。

学生分组：2 人/组。

2. 实训目的

通过实训，熟练掌握交换机端口安全配置基本操作。

3. 实训环境

（1）安装有 Windows 系统、网络监听软件（Wireshark）、MAC 地址修改软件（Mac

MakeUp)的 PC,每组 3 台。

(2) Cisco 二层交换机,每组 2 台。或者 Cisco 二层交换机,每组 1 台,其他集线器或交换机,每组 1 台。

(3) UTP 直通电缆,每组 2 条。

(4) UTP 交叉电缆,每组 1 条。

(5) Console 电缆,每组 1 条。

注意保持所有的交换机、路由器为出厂配置。

4. 实训准备

实训开始前按照图 3-26 所示网络拓扑连接好网络,其中,Switch1 为一台 Cisco 二层交换机,可用于模拟图 3-1 中网络中心(VLAN100)接入交换机和行政管理部(VLAN200)接入交换机的端口安全配置;另外一台交换机或集线器与计算机 PCa 一起用于模拟网络攻击设备;PCb 模拟被攻击的合法主机,PCc 模拟合法主机,主要用于验证网络连通性。

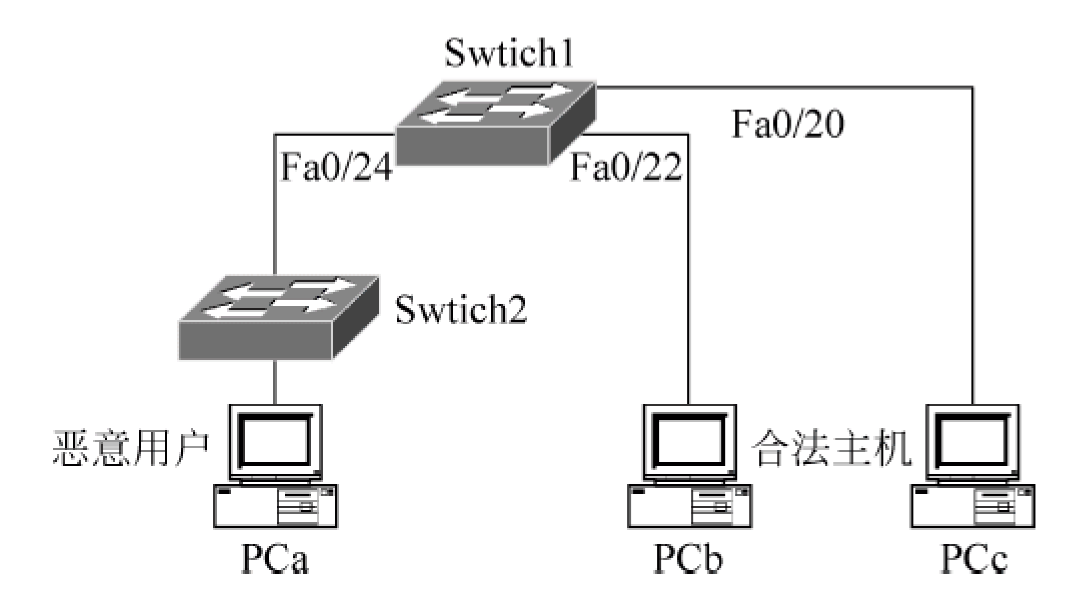


图 3-26 端口安全实训拓扑示意图

按照表 3-31 中所示为网络中 3 台主机配置好 IP 地址,并在实训前检查保证网络连通性。

表 3-31 端口安全实训主机 IP 地址

设 备	IP 地址/网络前缀	设 备	IP 地址/网络前缀
PCa	200.100.8.2/26	PCc	200.100.8.4/26
PCb	200.100.8.3/26		

为模拟 MAC 攻击,可以使用免费 MAC 地址修改软件 Mac MakeUp。该软件官方网站为 http://www.gorlani.com/publicprj/macmakeup/macmakeup.asp,下载后使用 winrar 释放,然后直接运行 MacMakeUp.exe 即可。

5. 实训内容

(1) 动态获得安全 MAC 地址配置。

(2) MAC 地址泛洪攻防模拟。

(3) 粘性获得安全 MAC 地址配置。

(4) MAC 地址欺骗攻防模拟。

6. 实训指导

(1) 配置交换机端口安全防御

启动 Switch1，并使用 console 方式参考 3.3.3 小节中网络中心接入交换机端口安全配置方案对其进行配置。配置命令如下。

```
Switch1(config)# vlan  10
Switch1(config-vlan)# name  nic
Switch1(configv-vlan)# exit
Switch1 (config)# interface  range  fa0/22  -  24
Switch1(config-if-range)# switchport  mode  access
Switch1(config-if-range)# switchport  access  vlan  100
Switch1(config-if-range)# switchport  port-security
Switch1(config-if-range)# switchport  port-security  maximum  1
Switch1(config-if-range)# switchport  port-security  mac-address  sticky
Switch1(config-if-range)# switchport  port-security  violation  restict
Switch1(config-if-range)# switchport  block  unicast
Switch1(config-if-range)# switchport  block  multicast
Switch1(config-if-range)# exit
Switch1(config)# mac-address-table  static  0000.0000.0000  vlan  100  drop
```

配置完成后，在 PCa 上 CMD 命令行窗口中输入 ping　200.100.8.3 命令，使网络上产生 PCa 和 PCb 的流量，此时应能 ping 通。然后在连接到交换机 Switch1 的终端窗口中输入 **show　port-security　address** 命令，应能查看到交换机已经学习到 PCa、PCb 两台计算机的安全 MAC 地址。

```
Switch1# show  port-security  address
              Secure Mac Address Table
---------------------------------------------------
Vlan     Mac Address       Type           Ports    Remaining Age
                                                    (mins)
----     ----------        -----          ------   ------------
100      0015.58d3.0d5b    SecureSticky   Fa0/22   -
100      0015.5886.bcec    SecureSticky   Fa0/24   -
---------------------------------------------------
Total Addresses in System (excluding one mac per port)      : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

(2) MAC 地址泛洪攻击模拟

本操作使用 MAC 地址修改软件对 PCa 的 MAC 地址进行多次修改，模拟 MAC 地址泛洪攻击。

注意：为使修改的 MAC 地址生效，Mac MakeUp 会自动重启网卡。而对于动态学习安全 MAC 地址的交换机，端口重启会清除 MAC 地址表条目，所以必须在 PCa 与 Switch1 间连接一个交换机或集线器，以防止 PCa 网卡重启清除 Switch1 上动态学习的安全 MAC 地址条目。

首先运行 MacMakeUp.exe，打开图 3-27 所示界面。

在图 3-27 中 1 处下拉列表框中选择要修改 MAC 地址的网卡，图中所示为选择了 PCa 主机上的一块 PCI 网卡。

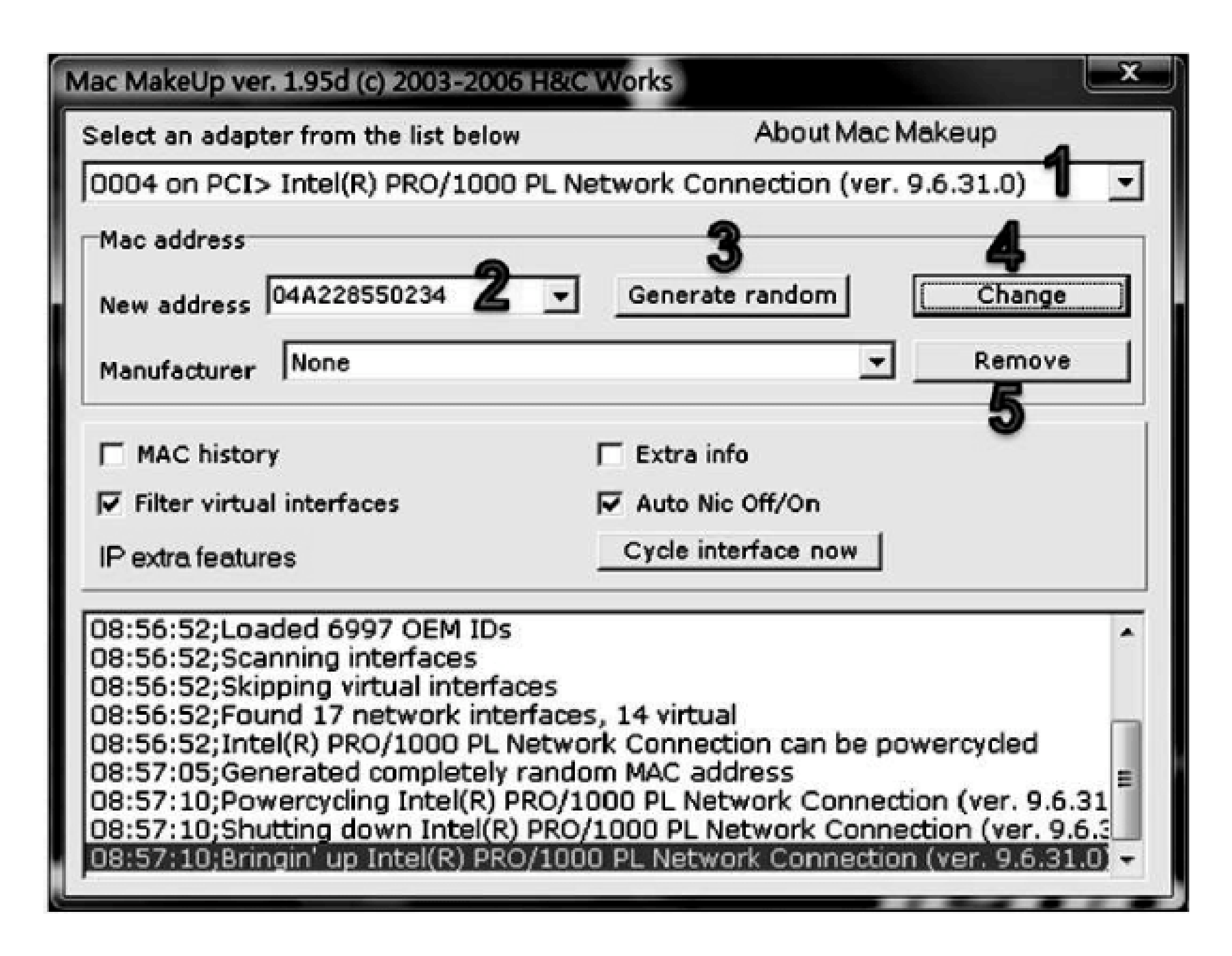


图 3-27　Mac MakeUp 运行界面

单击 3 处的 Generate random 按钮，在图 3-28 弹出菜单中选择 Completely random MAC 命令随机生成一个 MAC 地址，该地址会在图 3-27 中 2 处的下拉列表框中显示。



图 3-28　Mac MakeUp 随机生成 MAC 弹出菜单

单击图 3-27 中 4 处的 Change 按钮改变所选网卡的 MAC 地址，然后在 PCa 机 CMD 命令行窗口中使用 ipconfig/all 命令检查应能发现 MAC 地址已经被修改，如图 3-29 所示。



图 3-29　ipconfig /all 命令检查网卡 MAC 地址

根据目前端口安全配置，端口 Fa0/24 只允许前面粘性获得的安全 MAC 地址流量通过，此时 MAC 地址改变，会在该端口上发生违规行为，交换机端口不会关闭，但会随即在终端窗口中显示违规通知。限制模式违规通知示例如下。

```
01:00:55: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused
by MAC address 04a2.2855.0234 on port FastEthernet0/24.
```

此时在 PCb 上使用 ping 200.100.8.2 命令测试网络连通性，应发现不能 ping 通，但使用 ping 200.100.8.4，能够 ping 通 PCc。

在交换机 Switch1 上使用 show mac-address-table 命令检查当前 MAC 地址表，会发现，不管使用 Mac MakeUp 如何改变 PCa 的 MAC 地址，在交换机 MAC 地址表中 Fa0/24 端口对应的都只有一条粘性获得的安全 MAC 地址。

```
Switch1#show mac-address-table
          Mac Address Table
-------------------------------
此处省略部分显示...
Vlan    Mac Address       Type        Ports
----    ----------        ------      ----
All     ffff.ffff.ffff    STATIC      CPU
100     0000.0000.0000    STATIC      Drop
此处省略部分显示...
100     0015.5886.bcec    STATIC      Fa0/24
100     0015.58d3.0d5b    STATIC      Fa0/22
Total Mac Addresses for this criterion: 23
```

为对比使用端口安全前后效果，可先在交换机 Switch1 上进行下面所示操作停用 Fa0/24 端口安全特性。然后使用 Mac MakeUp 多次改变 PCb 的 MAC 地址后再检查 MAC 地址表，此时会发现多条 Fa0/24 端口的 MAC 地址条目，重复使用 Mac MakeUp 修改 PCb 的 MAC 地址，会发现交换机对端口对应的 MAC 地址条目不再有限制。

```
Switch1(config)#interface fa0/24
Switch1(config-if)#no switchport port-security
Switch1(config-if)#end
Switch1#show mac-address-table
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
此处省略若干显示...
All     ffff.ffff.ffff    STATIC      CPU
  100   0000.0000.0000    STATIC      Drop
此处省略若干显示...
  100   0015.5886.bcec    DYNAMIC     Fa0/24
  100   0015.58d3.0d5b    DYNAMIC     Fa0/22
  100   04a2.2855.0234    DYNAMIC     Fa0/24
  100   4246.df49.8780    DYNAMIC     Fa0/24
```

```
  100     6e33.77f2.fcbc     DYNAMIC     Fa0/24
Total Mac Addresses for this criterion: 26
```

(3) 粘性获得安全 MAC 地址配置

重新启动或重载 Switch1,并使用 console 方式参考 3.5.3 小节中研发部接入交换机端口安全配置方案对其进行配置。配置命令如下。

```
Switch1(config)#vlan 200
Switch1(config-vlan)#name res
Switch1(config-vlan)#exit
Switch1(config)#interface range fa0/22 - 24
Switch1(config-if-range)#switchport mode access
Switch1(config-if-range)#switchport access vlan 200
Switch1(config-if-range)#switchport port-security
Switch1(config-if-range)#switchport port-security maximum 1
Switch1(config-if-range)#switchport port-security violation shutdown
Switch1(config-if-range)#switchport block unicast
Switch1(config-if-range)#switchport block multicast
Switch1(config-if-range)#switchport port-security aging type inactivity
Switch1(config-if-range)#switchport port-security aging time 3
Switch1(config-if-range)#exit
Switch1(config)#mac-address-table static 0000.0000.0000 vlan 200 drop
Switch1(config-vlan)#exit
Switch1(config)#errdisable recovery cause psecure-violation
Switch1(config)#errdisable recovery interval 300
```

配置完成后,在 PCa 上 CMD 命令行窗口中输入 ping 200.100.8.3 命令,使网络上产生 PCa 和 PCb 的流量,此时应能 ping 通。然后在连接到交换机 Switch1 的终端窗口中使用 show port-security address 命令检查交换机应已经学习到 PCa、PCb 两台计算机的安全 MAC 地址,显示结果如下。

```
Switch1#show port-security address
                Secure Mac Address Table
-------------------------------------------------------------------------
Vlan      Mac Address        Type                    Ports      Remaining Age
                                                                       (mins)
----      -----------        ----                    -----      -------------
200       0015.58d3.0d5b     SecureDynamic           Fa0/22     300 (I)
200       0015.5886.bcec     SecureDynamic           Fa0/24     300 (I)
-------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)      : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

此时使用 Mac MakeUp 修改 PCa 的 MAC 地址,交换机会自动关闭 Fa0/24 端口,并在终端窗口显示如下所示违规通知。

```
Switch1#
00:50:42: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/24, putting Fa0/24 in
err-disable state
```

00:50:42: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0ab2.562e.f78c on port FastEthernet0/24.
00:50:43: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down
00:50:44: %LINK-3-UPDOWN: Interface FastEthernet0/24, changed state to down

不做任何操作,等待 3 分钟后,由于配置的 errdisable 计时器到时,交换机端口 Fa0/24 应能重新启用。errdisable 计时器到时端口重启显示如下。

00:55:03: %PM-4-ERR_RECOVER: Attempting to recover from psecure-violation err-disable state on Fa0/24
00:55:07: %LINK-3-UPDOWN: Interface FastEthernet0/24, changed state to up
00:55:08: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

(4) MAC 地址欺骗攻防模拟

如前所述,进行 MAC 地址欺骗攻击前,恶意用户首先要获取被攻击者的 MAC 地址。获取网络上主机 MAC 地址的方法很多,例如可以使用网络监听软件通过抓取数据包的方式获得。本实训操作模拟主机 PCa 上的恶意用户对 PCb 进行 MAC 地址欺骗攻击。

在 PCa 上运行 Wireshark 网络监听软件,模拟恶意用户获取网络上主机 MAC 地址。Wireshark 网络监听软件运行界面如图 3-30 所示。

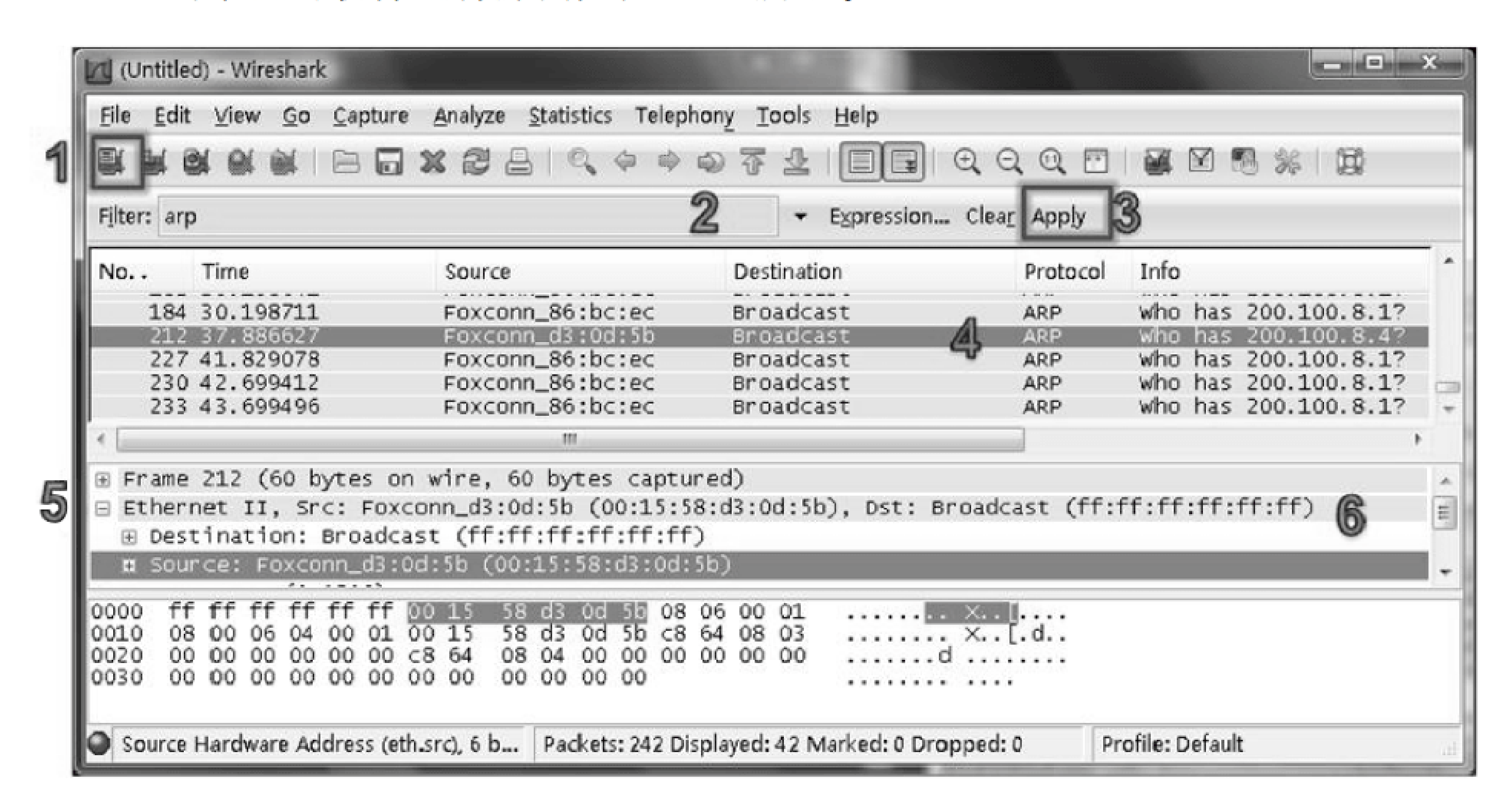


图 3-30　Wireshark 主窗口

单击图 3-30 主窗口中 1 处图标,打开图 3-31 所示窗口选择要监听的网卡。单击要监听的网卡列表项右端的 Start 按钮,启动监听。

然后在图 3-30 所示窗口中 2 处输入 arp 过滤字符串,即过滤只显示 ARP 流量。单击窗口中 3 处的 Apply 按钮应用该过滤字符串,则图 3-30 中 4 处子窗口中将只显示经过 PCa 网卡的 ARP 流量。



图 3-31 Wireshark 监听网卡窗口

在 PCc 上清空 ARP 缓存,然后 ping PCb,由于 ARP 请求采用广播包发送,所以在 PCa 上使用 Wireshark 也能从网卡上捕获到该数据包,并从中获得 PCc 的 MAC 地址。

在图 3-30 中 4 处子窗口中选择一个数据包,则在图中 6 处子窗口中会显示该数据包的逐层封装结构。

单击图 3-30 中 5 处,即二层数据帧封装,则会展开该数据帧,能看到该数据帧源 MAC 为 00:15:58:d3:0d:5b。

使用 Mac MakeUp 软件对配置了端口安全的交换机模拟进行一次 MAC 地址欺骗攻击。

首先在图 3-30 中 2 处,输入抓取的 PCb 的 MAC 地址 00:15:58:d3:0d:5b,然后单击 Change 按钮改变 PCa 主机的 MAC 地址。

此时,由于配置了端口安全特性,因此在交换机终端窗口中,会出现前面所述的端口被关闭通知,并且由于 Fa0/24 端口所接主机的 MAC 地址与已有的 Fa0/22 端口相同,Fa0/24 端口在 3 分钟 errdisable 到时重启后马上又进入 errdisable 状态,依旧不能启用。因此可以证明交换机端口安全可以阻挡 MAC 地址欺骗攻击。

模拟在没有配置端口安全的情况下,再进行一次 MAC 地址欺骗攻击。

进行模拟攻击前,使用 no switchport port-security 关闭交换机 Switch1 Fa0/24、Fa0/22 端口上端口安全特性,恢复 PCb 的真实 MAC 地址,保持 PCa、PCb、PCc 间的网络连通性。

使 PCc ARP 地址表中保存主机 PCb 的 MAC 地址 00:15:58:d3:0d:5b 与 IP 地址 200.100.8.4 间正确对应关系,在 PCc CMD 窗口中输入 arp-a 命令,应能看到该对应关系。

在 PCa 上运行 Wireshark 软件监听 ICMP 包,在 PCb CMD 窗口中输入 ping 200.100.8.4,由于 ICMP 数据流为单播流量,所以 PCa 上监听不到 PCc 与 PCb 的 ICMP 流量。

使用 Mac MakeUp 软件修改 PCa 的 MAC 地址为 00:15:58:d3:0d:5b,拔掉再插上 PCb 的网线,此时检查交换机 MAC 地址表会出现如下所示现象,即交换机会将端口 Fa0/24 主机 MAC 误认为是 00:15:58:d3:0d:5b。

```
Switch1#show  mac-address-table
          Mac Address Table
```

```
-------------------------------------------

Vlan      Mac Address        Type          Ports
----     -----------       --------      -----
All     ffff.ffff.ffff     STATIC        CPU
此处省略了部分显示...
  200      0015.58d3.0d5b     DYNAMIC      Fa0/24
Total Mac Addresses for this criterion: 21
```

在 PCa 上再次使用 Wireshark 进行监听。并在 PCc 上 CMD 窗口中输入 ping 200.100.8.4，由于交换机被欺骗，所以此时应能在 PCa 上收到交换机转发来的 ICMP 单播流量。

7. 实训报告

<table>
<tr><td>主机 MAC 地址</td><td>PCa:</td><td></td><td>PCb:</td><td></td><td>PCc:</td><td></td></tr>
<tr><td colspan="7">对 Switch1 模拟网络中心接入交换机端口安全配置后，填写下列 show 命令输出结果，并解释含义。</td></tr>
<tr><td colspan="7">(1) show port-security interface fa0/24 命令输出</td></tr>
<tr><td colspan="2">项</td><td colspan="2">值</td><td colspan="3">含义</td></tr>
<tr><td colspan="2">Port Security:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Port Status:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Violation Mode:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Aging Time:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Aging Type:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">SecureStatic Address Aging:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Maximum MAC Addresses:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Total MAC Addresses:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Configured MAC Addresses:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Sticky MAC Addresses:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Last Source Address: Vlan:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Security Violation Count:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="7">(2) show port-security interface fa0/22 命令输出</td></tr>
<tr><td colspan="2">项</td><td colspan="2">值</td><td colspan="3">含义</td></tr>
<tr><td colspan="2">Port Status:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Violation Mode:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Aging Time:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Aging Type:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">SecureStatic Address Aging:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Maximum MAC Addresses:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Total MAC Addresses:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Configured MAC Addresses:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Sticky MAC Addresses:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Last Source Address:Vlan:</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">Security Violation Count:</td><td colspan="2"></td><td colspan="3"></td></tr>
</table>

3.11.3 局域网 IEEE 802.1x 配置

1. 实训组织

实训学时：50 分钟。

学生分组：2 人/组。

2. 实训目的

通过实训，熟练掌握局域网 IEEE 802.1x 配置基本操作，理解 IEEE 802.1x 工作原理。

3. 实训环境

(1) 安装有 Windows 系统、网络监听软件(Wireshark)、FreeRADIUS.net 软件的 PC，每组 3 台。

(2) Cisco 二层交换机，每组 1 台。

(3) UTP 直通电缆，每组 3 条。

(4) Console 电缆，每组 1 条。

注意保持所有的交换机、路由器为出厂配置。

4. 实训准备

按照图 3-32 所示拓扑连接网络，按照表 3-32 配置各设备及主机的 IP 地址，并参考 3.2.3 小节配置启动 RADIUS 服务器。

注意：这里为了降低对网络设备要求，所有设备均分配同一个网络内 IP 地址。

表 3-32 IEEE 802.1x 实训 IP 地址分配

网络接口	IP/网络前缀	网络接口	IP/网络前缀
C2960-0-3-1 的管理 VLAN 虚接口：vlan99	200.100.8.1/26	PC-0-3-1	200.100.8.2/26
RAD-0-1-1	200.100.8.30/26	PC-0-3-2	200.100.8.3/26

图 3-32 中仅配置交换机 Fa0/24 端口和主机 PC-0-3-1 使用 IEEE 802.1x 进行身份验证，而端口 Fa0/23 和 PC-0-3-2 不做 IEEE 802.1x 配置，仅用于实训过程中测试网络连通性。

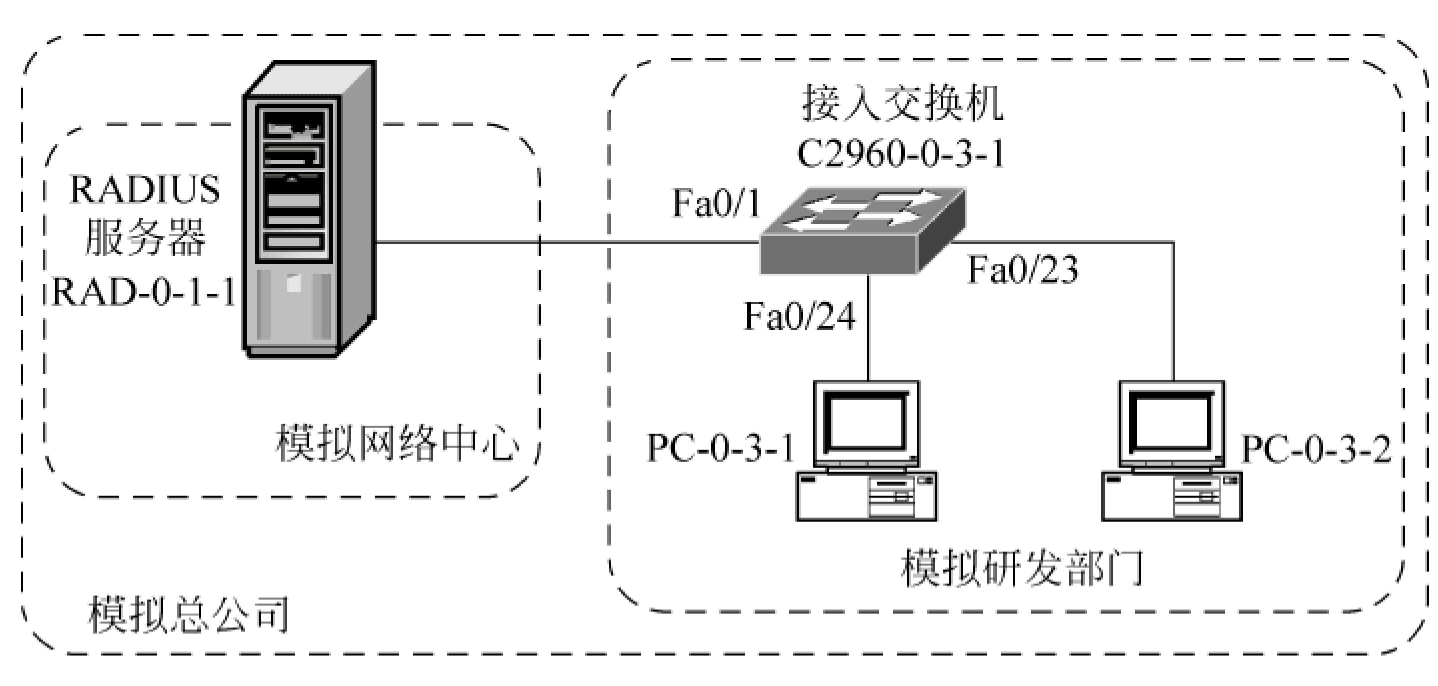


图 3-32 局域网 IEEE 802.1x 配置实训

5. 实训内容

（1）局域网交换机、主机的 IEEE 802.1x 配置。

（2）IEEE 802.1x 协议分析。

6. 实训指导

（1）检查网络连通性以及 RADIUS 服务可用性。

在配置交换机的 IEEE 802.1x 安全特性前，使用 ping 命令检查网络连通性。在保证从 RADIUS 服务器可以成功 ping 通各 PC 的基础上，启动 RADIUS 服务器，然后使用 netstat 命令检查 RADIUS 服务器是否已经打开 1812、1813 端口监听请求。

（2）局域网接入交换机网络连接配置如下。

```
C2960-0-3-1(config)#vlan 99                                                    ①
C2960-0-3-1(config-vlan)#name mgmt
C2960-0-3-1(config-vlan)#exit
C2960-0-3-1(config)#interface fa0/1
C2960-0-3-1(config-if)#switchport mode trunk                                   ②
C2960-0-3-1(config-if)#switchport trunk native vlan 99
00:39:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down
00:39:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
C2960-0-3-1(config)#interface vlan 99                                          ③
C2960-0-3-1(config-if)#interface vlan 99
C2960-0-3-1(config-if)#ip add 200.100.8.1 255.255.255.192
```

其中：

① 创建管理 VLAN。

② 将接入交换机的上联端口配置为干道模式，并配置交换机的本征 VLAN 为 99。此步配置模拟接入交换机上联汇聚交换机。

③ 为管理 VLAN 虚接口配置 IP 地址。

（3）局域网交换机、主机的 IEEE 802.1x 配置。

在局域网交换机 Fa0/24 端口上配置启用 IEEE 802.1x，操作如下所示。

```
C2960-0-3-1(config)#aaa new-model                                              ①
C2960-0-3-1(config)#aaa authentication dot1x default group radius              ②
C2960-0-3-1(config)#radius-server host 200.100.8.30 auth-port 1812 acct-port 1813 timeout 1
retransmit 3                                                                   ③
C2960-0-3-1(config)#radius-server key Net&Sec@sjzpc                            ④
C2960-0-3-1(config)#dot1x system-auth-control                                  ⑤
C2960-0-3-1(config)#interface fa0/24
C2960-0-3-1(config-if)#switchport mode access                                  ⑥
C2960-0-3-1(config-if)#dot1x port-control auto                                 ⑦
C2960-0-3-1(config-if)#dot1x pae authenticator                                 ⑧
```

其中：

① 启用交换机 AAA 安全特性。

② 定义 IEEE 802.1x 身份验证默认方法为到 RADIUS 服务器上进行验证，如果失败则使用本地数据库进行身份验证。

③ 定义 RADIUS 服务器有关信息。

④ 定义 RADIUS 服务器与客户端的共享密钥。

⑤ 定义交换机启用 IEEE 802.1x 安全特性。

⑥ 定义端口工作模式为接入模式。

⑦ 配置在当前端口上启用 IEEE 802.1x，并使端口根据交换机与客户端之间的 IEEE 802.1x 认证情况迁移到已授权或未授权状态。

⑧ 定义端口启用 IEEE 802.1x 认证。

(4) IEEE 802.1x 配置检查及调试。

首先在交换机上使用 debug dot1x all 命令打开交换机的 IEEE 802.1x 身份验证调试信息。

然后在 PC-0-3-1 上修改网络连接属性，参考 3.4.2 小节启用 IEEE 802.1x 身份验证并配置身份验证参数。

此时如果将 PC-0-3-1 连接到交换机，则在 Windows 系统托盘的网络连接处会出现提示信息，如图 3-33 所示。

单击对应图标，则弹出 IEEE 802.1x 身份验证窗口，如图 3-34 所示。在该窗口中输入在 RADIUS 服务器上已经注册的用户名、口令，单击“确定”按钮，进行认证。如果身份验证成功，则网络连接进入连通状态。

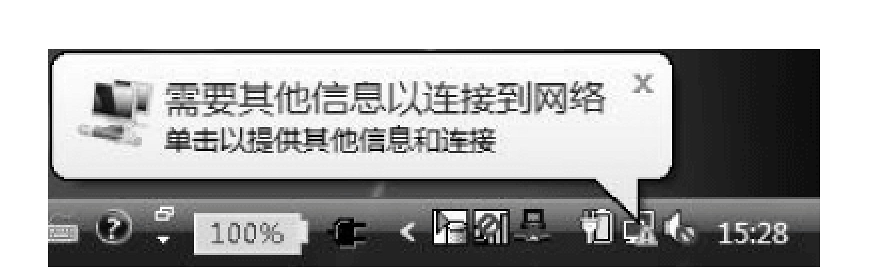


图 3-33 Windows 网络连接 IEEE 802.1x 认证提示信息



图 3-34 Windows IEEE 802.1x 身份验证窗口

(5) 分析 IEEE 802.1x 协议。

分别在 RADIUS 服务器和 PC0-3-1 上启动 Wireshark 软件，抓取 RADIUS 协议报文和 EAP 消息。注意可在 Wireshark 数据过滤窗口中输入 eap 来过滤 EAP 消息，如图 3-35 所示。

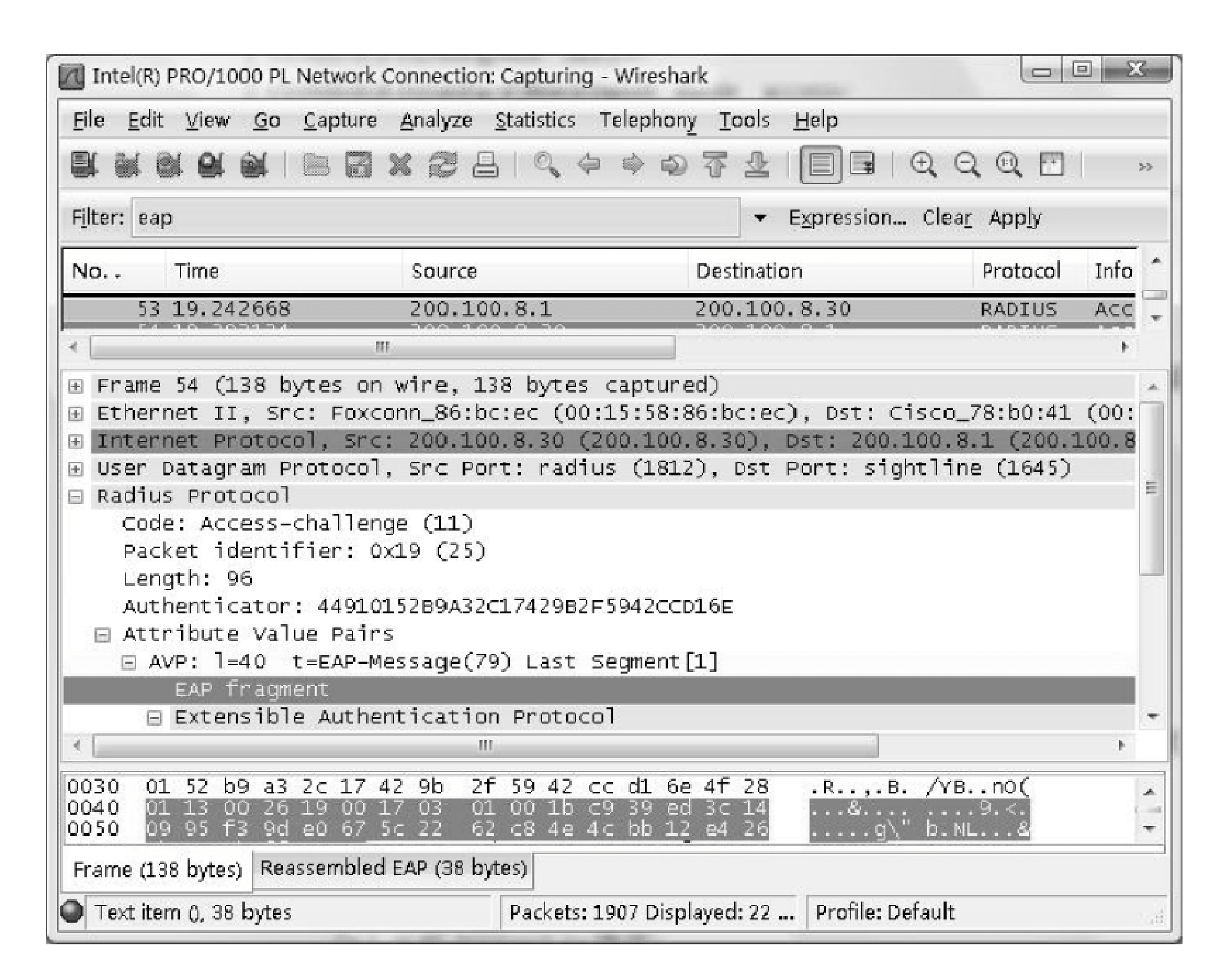


图 3-35　RADIUS 内封装 EAP 消息示例

7. 实训报告

配置 IEEE 802.1x 后，使用 show dot1x interface fa0/24 显示交换机 C2960-0-3-1 Fa0/24 端口的状态及相应含义。

状态参数	值	含　义
PAE		
PortControl		
ControlDirection		
HostMode		
ReAuthentication		

分析使用 Wireshark 抓到的 EAP 消息，回答以下问题。

1. PC-0-3-1 与交换机之间的 EAP 消息，外层封装是什么协议？

2. PC-0-3-1 与交换机之间进行身份验证分别使用了下列哪些 EAP 消息？按出现顺序将其填写在下表中。

EAP 认证阶段	序　号	EAP 消息类型
初始化认证		
开始认证		
结束网络连接		

续表

3. RADIUS 服务器与交换机间的 EAP 消息，外层封装是什么协议？
4. 对比 RADIUS 服务器与交换机间传输的 EAP 消息，以及 PC-0-3-1 与交换机间传输的 EAP 消息的时间、内容，回答问题。 (1) 交换机是否对 PC-0-3-1 发来的 EAP 消息进行了修改后发送给 RADIUS 服务器？ (2) PC-0-3-1 提交的用户名、口令是否在网络上明文传输了？

3.11.4 局域网交换机访问控制

1. 实训组织

实训学时：100 分钟。

学生分组：2 人/组。

2. 实训目的

通过实训，熟练掌握局域网交换机上 VACL、PACL 配置操作。

3. 实训环境

(1) 安装有 Windows 系统、网络监听软件（Wireshark）、网络服务软件（例如 XAMPP）的 PC，每组 2 台。

(2) Cisco 二层交换机，每组 1 台。

(3) Cisco 三层交换机，每组 1 台。

(4) UTP 直通电缆，每组 4 条。

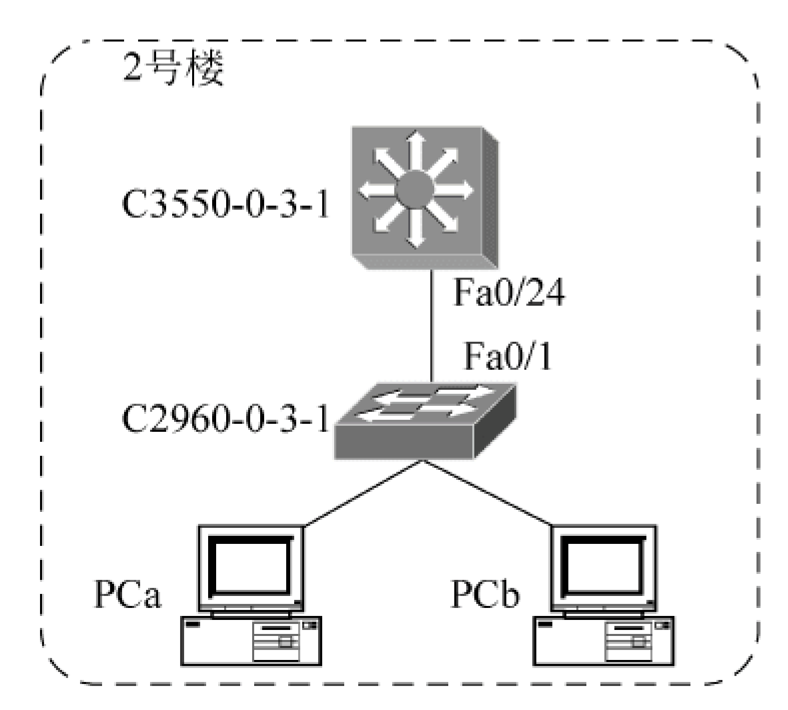
(5) UTP 交叉电缆，每组 1 条。

(6) Console 电缆，每组 2 条。

注意保持所有的交换机为出厂配置。

4. 实训准备

按照图 3-36 所示模拟公司总部局域网简化拓扑示意图搭建实训环境。图中 C3550-0-3-1 模拟生产部、市场部、研发部网络的汇聚交换机，C2960-0-3-1 分别模拟生产部网络接入交换机和总部 2 号楼的市场部接入交换机和研发部接入交换机。PCa、PCb 分别模拟网络中的 PC 机和服务器。按照图中下方表格中信息完成 C3550-0-3-1 和 C2960-0-3-1 上网络连接与 VLAN、路由等配置。



VLAN号	VLAN名	IP	网络	C2960-3-1端口
300	res&dev	200.100.9.0/24	研发部	Fa0/9、Fa0/10
400	market	200.100.10.0/25	市场部	Fa0/15、Fa0/16
600	workshop	200.100.11.0/24	厂房	Fa0/23、Fa0/24

图 3-36　VACL 配置实训示例

5. 实训内容

（1）VACL 配置。

（2）基于 IP 访问控制列表的 PACL 配置。

（3）基于 MAC 扩展访问控制列表的 PACL 配置。

6. 实训指导

（1）VACL 配置

用 C3550-0-3-1 模拟生产部汇聚交换机，参考如下所示配置基于 IP 访问控制列表的 VACL，用 C2960-0-3-1 模拟生产部、市场部接入交换机，用主机 PCa 模拟生产部前置机，PCb 分别模拟生产主机和市场部普通主机测试配置的 VACL 能否正常工作。注意将 PCa、PCb 连接到正确的交换机端口上，并在配置访问控制列表前测试网络连通性，以及能否正常访问网络服务（例如使用 XAMPP 提供的 Web 服务、FTP 服务等）。

```
C3550-0-3-1(config)# ip access-list extended eacl-vacl-60
C3550-0-3-1(config-ext-nacl)# permit icmp any any
C3550-0-3-1(config-ext-nacl)# permit ip any 200.100.11.0 0.0.0.31
C3550-0-3-1(config-ext-nacl)# permit ip 200.100.11.0 0.0.0.31 any
C3550-0-3-1(config-ext-nacl)# permit ip 200.100.11.0 0.0.0.255 200.100.11.0 0.0.0.255
C3550-0-3-1(config-ext-nacl)# exit
C3550-0-3-1(config)# vlan access-map vam-60 10
C3550-0-3-(config-access-map)# match ip address eacl-vacl-60
C3550-0-3-(config-access-map)# action forward
C3550-0-3-(config-access-map)# exit
C3550-0-3-1(config)# vlan access-map vam-60 20
C3550-0-3-(config-access-map)# match ip address sacl-vacl-60
C3550-0-3-(config-access-map)# action drop
C3550-0-3-(config-access-map)# exit
```

```
C3550-0-3-1(config)# vlan filter vam-60 vlan-list 60
C3550-0-3-1(config)# exit
```

(2) 基于 IP 访问控制列表的 PACL 配置

用 C3550-0-3-1 模拟研发部汇聚交换机，用 C2960-0-3-1 模拟研发部接入交换机，参考如下所示配置基于 IP 访问控制列表的 PACL，用主机 PCa 模拟研发部服务器和研发部普通主机，PCb 分别模拟研发部普通主机和市场部普通主机测试配置的 PACL 能否正常工作。注意将 PCa、PCb 连接到正确的交换机端口上，并在配置访问控制列表前测试网络连通性，以及能否正常访问网络服务(例如使用 XAMPP 提供的 Web 服务、FTP 服务等)。

```
C2960-0-3-1(config)# ip access-list extended eacl-pacl-30
C2960-0-3-1(config-ext-nacl)# permit ip any 200.100.9.0 0.0.0.7
C2960-0-3-1(config-ext-nacl)# permit tcp any 200.100.9.0 0.0.0.255 established
C2960-0-3-1(config-ext-nacl)# deny tcp any 200.100.9.0 0.0.0.255
C2960-0-3-1(config-ext-nacl)# deny udp any 200.100.9.0 0.0.0.255 eq netbios-ns
C2960-0-3-1(config-ext-nacl)# permit ip any any
C2960-0-3-1(config-ext-nacl)# exit
C2960-0-3-1(config)# interface range fa0/9 - 10
C2960-0-3-1(config-if-range)# ip access-group eacl-pacl-30 in
C2960-0-3-1(config-if-range)#
```

用 C3550-0-3-1 模拟市场部汇聚交换机，用 C2960-0-3-1 模拟市场部接入交换机，参考如下所示配置基于 IP 访问控制列表的 PACL，用主机 PCa 模拟市场部服务器和市场部普通主机，PCb 分别模拟市场部普通主机和研发部普通主机测试配置的 PACL 能否正常工作。注意将 PCa、PCb 连接到正确的交换机端口上，并在配置访问控制列表前测试网络连通性，以及能否正常访问网络服务(例如使用 XAMPP 提供的 Web 服务、FTP 服务等)。

```
C2960-0-3-1(config)# ip access-list extended eacl-pacl-40
C2960-0-3-1(config-ext-nacl)# permit ip any 200.100.10.0 0.0.0.7
C2960-0-3-1(config-ext-nacl)# permit tcp any 200.100.10.0 0.0.0.127 established
C2960-0-3-1(config-ext-nacl)# deny tcp any 200.100.10.0 0.0.0.127
C2960-0-3-1(config-ext-nacl)# deny udp any 200.100.10.0 0.0.0.127 eq netbios-ns
C2960-0-3-1(config-ext-nacl)# permit ip 200.100.10.0 0.0.0.7 any
C2960-0-3-1(config-ext-nacl)# permit icmp any any
C2960-0-3-1(config-ext-nacl)# deny ip 200.100.10.0 0.0.0.127 200.100.10.0 0.0.
0.127
C2960-0-3-1(config-ext-nacl)# permit ip any any
C2960-0-3-1(config-ext-nacl)# exit
C2960-0-3-1(config)# interface range fa0/15 - 16
C2960-0-3-1(config-if-range)# ip access-group eacl-pacl-40 in
C2960-0-3-1(config-if-range)#
```

(3) 基于 MAC 扩展访问控制列表的 PACL 配置

用 C2960-0-3-1 模拟市场部接入交换机，将 PCa、PCb 连接到正确的交换机端口上。用主机 PCa 模拟网络中普通主机，在 PCb 上使用类似 Winarpattacker 软件向网络中发动 ARP 洪水攻击。观察 PCa 上被攻击后现象，并参考如下配置基于 MAC 扩展访问控制列表的 PACL，过滤 PCb 所在端口发出的 ARP 流量，用 Wireshark 软件观察 ARP 流量

情况。

```
C2960-0-3-1(config)# mac access-list extended macl-pacl-arp
C2960-0-3-1(config-ext-macl)# deny host xxxx.xxxx.xxxx any 0x806 0x0
C2960-0-3-1(config-ext-macl)# exit
C2960-0-3-1(config)# interface fa0/15
C2960-0-3-1(config-if)# mac access-group macl-pacl-arp in
```

7. 实训报告

记录实训网络连接配置情况：

	IP 地址/网络前缀	网关 IP	C2960-0-3-1 交换机端口号	所属 VLAN
生产部前置机				
生产部普通主机				
研发部服务器				
研发部主机				
市场部服务器				
市场部主机				

检测内容	结果		测试手段/问题分析
网络连接完成后，连通性测试结果：			
将 PCa 与 PCb 模拟各部网络服务器与普通主机接入交换机，它们能否相互 ping 通？	通 □	不通 □	
生产部主机能否 ping 通其他市场部、研发部网关？	通 □	不通 □	
启动服务器程序，普通主机能否访问服务器？	可以 □	不可以 □	
配置 VACL 后测试结果：			
生产部主机能否访问生产部前置机上的网络服务？	可以 □	不可以 □	
市场部主机能否访问生产部前置机上的网络服务？	可以 □	不可以 □	
市场部主机能否访问生产部主机上的网络服务？	可以 □	不可以 □	
配置研发部 PACL 后测试结果：			
研发部主机能否访问研发部服务器上的网络服务？	可以 □	不可以 □	
研发部主机能否访问研发部其他主机上的网络服务？	可以 □	不可以 □	
市场部主机能否访问研发部服务器上的网络服务？	可以 □	不可以 □	
配置市场部 PACL 后测试结果：			
市场部主机能否访问市场部服务器上的网络服务？	可以 □	不可以 □	
市场部主机能否访问市场部其他主机上的网络服务？	可以 □	不可以 □	
研发部主机能否访问市场部服务器上的网络服务？	可以 □	不可以 □	
配置市场部过滤 MAC 的 PACL 后测试结果：			
被过滤的市场部主机能否 ping 通市场部服务器？	通 □	不通 □	
使用 Wireshark 观察另一市场部主机能否接收到被过滤主机的 ARP 报文？	可以 □	不可以 □	
使用 Wireshark 观察发送 ARP 请求洪水攻击数据包的内容。观察是否网络中所有主机均会接收并处理 ARP 请求广播？	所有主机 □	仅目的主机□	

3.11.5 DHCP 攻击、IP 地址欺骗攻击、ARP 攻击防护

1. 实训组织

实训学时：100 分钟。

学生分组：2 人/组。

2. 实训目的

通过实训熟练掌握局域网交换机上 DHCP 监听、IPSG、ARP 绑定配置操作。

3. 实训环境

(1) 安装有 Windows 系统、网络监听软件(Wireshark)、IP 欺骗攻击软件(例如 smurf)、ARP 攻击软件(例如 winarpattacker)、DHCP 服务软件的 PC，每组 3～4 台。

(2) Cisco 二层交换机(建议使用安装了 12.2(50)SE3 版本的 Cisco Catalyst 2960)，每组 1 台。

(3) DHCP 服务器，每组 1 台。

(4) UTP 直通电缆，每组 3～4 条。

(5) Console 电缆，每组 1 条。

注意保持所有的交换机为出厂配置。

4. 实训准备

按照图 3-37 所示模拟公司总部局域网的简化拓扑示意图搭建实训环境。C2960-0-3-1 模拟市场部网络所连接的某接入交换机。为简化实训环境要求，省略了汇聚交换机而将 DHCP 服务器直接连接到 C2960-0-3-1 的 Fa0/1 端口。

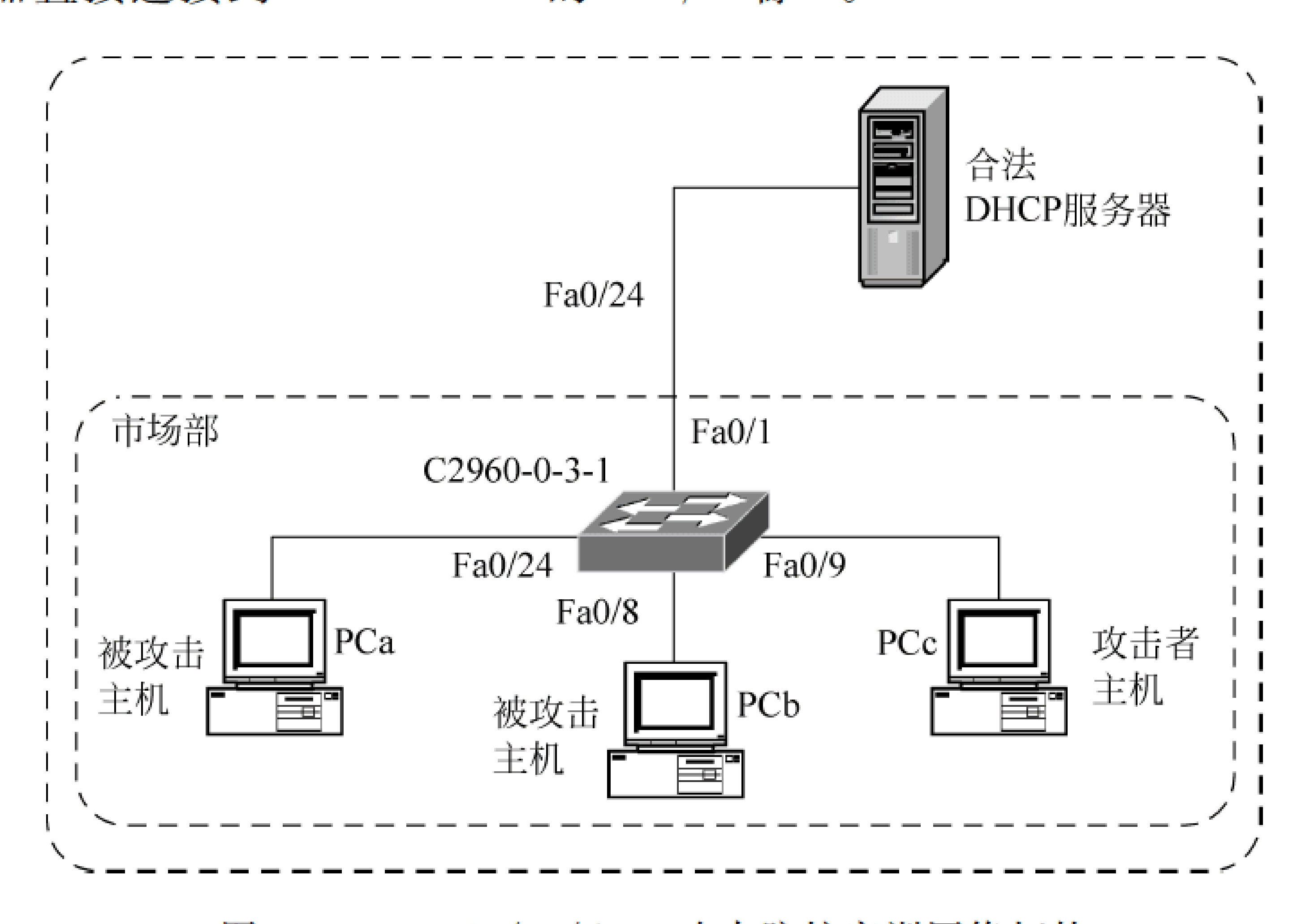


图 3-37 DHCP/IP/ARP 攻击防护实训网络拓扑

进行实训前需完成以下准备工作。

(1) 在 C2960-0-3-1 上创建市场部所在 VLAN300，并将相应端口分配到 VLAN300 中。注意，所有端口均应设置为接入模式。

(2) 为图 3-37 中合法 DHCP 服务器和 PCc 分别配置 IP 为 200.100.10.10 和

200.100.10.254，并将 PCa、PCb 配置为自动获得 IP 地址。

(3) 按如下要求，在 DHCP 服务器上配置 DHCP 服务地址池。

网络地址范围：200.100.10.0/25

网关地址：200.100.10.1

排除地址：200.100.10.1～200.100.10.7

(4) 按如下要求，在攻击者主机上配置 DHCP 服务地址池。

网络地址范围：200.100.10.0/24

网关地址：200.100.10.254

5. 实训内容

(1) DHCP 监听配置与 DHCP 攻击防护。

(2) IPSG 配置与 IP 欺骗攻击防护。

(3) DAI 配置与 ARP 攻击防护。

6. 实训指导

(1) DHCP 监听配置与 DHCP 攻击防护

在未对交换机进行 DHCP 监听配置前，启动 PCa 和 PCb，并在 PCa 和 PCb 运行 Wireshark 监听所有 bootp 协议报文，检查攻击者是否欺骗 PCa、PCb，使其获得了错误的 IP 地址。

在 C2960-0-3-1 上配置在 VLAN300 上启用 DHCP 监听，除 Fa0/1 端口配置为可信端口外，其他端口都配置为不可信端口，操作如下。

```
C2960-0-3-1(config)# ip dhcp snooping
C2960-0-3-1(config)# ip dhcp snooping vlan 300
C2960-0-3-1(config)# interface fa0/1
C2960-0-3-1(config-if)# ip dhcp snooping trust
C2960-0-3-1(config-if)# end
C2960-0-3-1# show ip dhcp snooping binding
MacAddress          IpAddress      Lease(sec)   Type           VLAN   Interface
--------------      ---------      ----------   -----------    ----   ---------------
00:15:58:86:BC:EC   200.100.10.3   85849        dhcp-snooping  300    FastEthernet0/24
F4:AA:3D:63:C7:59   200.100.10.4   85366        dhcp-snooping  300    FastEthernet0/8
Total number of bindings: 2
```

先禁用再启用 PCa 和 PCb，检查此时攻击者能否再假冒合法 DHCP 服务器欺骗 PCa、PCb。

(2) IPSG 配置与 IP 欺骗攻击防护

在未对交换机 C2960-0-3-1 配置 IPSG 前，重新禁用再启用 PCa、PCb 网络连接，保证其能获得正确 IP。

在 PCc 上运行 IP 欺骗攻击软件(例如 smurf)假冒 PCb 地址发送 ICMP 给网络中的 PCa，在 PCa、PCb 和 PCc 上运行 Wireshark 监测 smurf 攻击数据报文。此时在 PCb 上会收到 PCa 发送的 ICMP 响应报文，虽然 PCb 并没有 ping PCa。

在交换机 C2960-0-3-1 上配置端口 Fa0/2～Fa0/24 启用 IPSG。同时配置 PCb 的静

态 IP-MAC-端口绑定条目，如下所示。

```
C2960-0-3-1(config)# interface range fa0/2 - 24                                    ①
C2960-0-3-1(config-if-range)# ip verify source                                       ②
此处省略部分显示...
*Mar 1 02:22:29.576: IP_SOURCE_GUARD: get per port/vlan ip binding, port:
FastEthernet0/8, vlan: 300, number of bindings: 1.                                   ③
此处省略部分显示...
C2960-0-3-1(config-if-range)# exit
C2960-0-3-1(config)# ip source bind F4AA.3D63.C759 vlan 300 200.100.10.6
interface fa0/8                                                                      ④
C2960-0-3-1(config)# end
C2960-0-3-1#show ip source binding                                                   ⑤
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
-----------------   -------------   ----------  -------------  ----  ------------------
00:15:58:86:BC:EC   200.100.10.4    81092       dhcp-snooping  300   FastEthernet0/24
F4:AA:3D:63:C7:59   200.100.10.6    infinite    static         300   FastEthernet0/8
Total number of bindings: 2
```

以上各行操作配置的含义如下。

① 使用 interface range 命令批量配置端口。

② 在端口 Fa0/2～Fa0/24 上启用 IPSG。

③ 由于事先配置了 debug ip verify source packet，所以在端口 Fa0/8 上启用了 IPSG 后出现相应提示。

④ 配置 PCb 的静态绑定条目。

⑤ 配置完成后检查 IPSG 绑定情况，从输出结果可以看出 Fa0/8 的绑定类型为 static 即静态绑定。

完成以上配置后，再次由 PCc 运行 smurf 假冒 PCb 发送 ICMP 给 PCa，检查 PCa 是否收到该数据报文。

将 PCb 当做攻击主机，运行 smurf 假冒 PCc 发送 ICMP 请求报文给 PCa，检查 PCa 是否收到该数据报文。

(3) DAI 配置与 ARP 攻击防护

进行该实训任务前，恢复网络连通性。在 PCc 上运行 ARP 攻击软件(例如 Winarpattacker)，以 PCb 为攻击对象发动 IP 冲突攻击。在 PCb 上使用 Wireshark 观察网络连接是否受到了攻击影响。

停止攻击，在交换机 C2960-0-3-1 端口 Fa0/2～Fa0/24 上配置基于 DHCP 监听的 DAI 和 ARP 流量限制，如下所示。

```
C2960-0-3-1(config)# ip arp inspection vlan 300                                      ①
C2960-0-3-1(config)# interface range fa0/2 - 24
C2960-0-3-1(config-if-range)# ip arp inspection limit rate 50                        ②
C2960-0-3-1(config)# end
C2960-0-3-1# show ip arp inspection interfaces fa0/9                                 ③

Interface          Trust State    Rate (pps)   Burst Interval
---------------    -----------    ----------   --------------
```

```
Fa0/9                Untrusted     50                    1

C2960-0-3-1#show ip arp inspection vlan 300                          ④

Source Mac Validation        : Disabled
Destination Mac Validation   : Disabled
IP Address Validation        : Disabled

Vlan    Configuration    Operation    ACL Match        Static ACL
----    -------------    ---------    ---------        ---------
300      Enabled           Active

Vlan    ACL Logging      DHCP Logging        Probe Logging
----    -----------      ------------        -------------
300      Deny              Deny                Off
*Mar  1 03:04:26.796: %SW_DAI-4-PACKET_RATE_EXCEEDED: 65 packets received in 8
milliseconds on Fa0/9.                                                ⑤
*Mar  1 03:04:26.796: %PM-4-ERR_DISABLE: arp-inspection error detected on Fa0/9,
putting Fa0/9 in err-disable state                                    ⑥
*Mar  1 03:04:26.805: IP_SOURCE_GUARD: dhcp snooping vp state change, vlan: 300,
port: FastEthernet0/9, add flag: 0.                                   ⑦
*Mar  1 03:04:26.813: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/9, changed state to down                                ⑧
*Mar  1 06:01:24.802: %SW_DAI-4-DHCP_SNOOPING_DENY: 15 Invalid ARPs (Req) on
Fa0/9, vlan 300.([0000.0000.0001/200.100.10.1/0000.0000.0000/200.100.10.6/06:01:24
UTC Mon Mar 1 1993])                                                  ⑨
*Mar  1 03:04:28.809: %LINK-3-UPDOWN: Interface FastEthernet0/9, changed state to
down                                                                  ⑩
```

以上各行命令操作的含义如下。

① 在交换机上 VLAN300 上启用 DAI。

② 在端口 Fa0/2～Fa0/24 上启用 ARP 报文限速，速率限制为 50pps。

③ 检查端口 Fa0/9 上的 DAI 配置。图 3-37 中显示 Fa0/9 不是 ARP 的可信端口，端口限速 ARP 报文速率为 50pps。

④ 检查交换机 VLAN300 上 DAI 配置，可以发现 VLAN300 上已经启用了 DAI。

⑤ 在 PCc 上使用 ARP 攻击软件发出 ARP 攻击报文，交换机监测到端口 Fa0/9 上有过多 ARP 流量。

⑥ 由于检测到端口 Fa0/9 上有过多流量，端口被 down。

⑦ 端口被 down 后，端口 Fa0/9 上 DHCP 监听的状态改变，这个改变被端口上的 IPSG 监测到。

⑧ 端口 Fa0/9 链路协议进入 down 状态。

⑨ 端口 Fa0/9 上配置 DAI 同时监测到 15 个无效的 ARP 请求报文，该 ARP 报文中使用的源 IP 地址为 200.100.0.1，源 MAC 地址为 0000.0000.0001，而目标 MAC 地址为 0000.0000.0000，目标 IP 地址为 200.100.10.6。

⑩ 端口连接状态转变为 down。

配置完成后运行 DAI 检查命令，检查配置情况，并在 PCc 上运行 ARP 攻击软件，测

试配置是否起到作用。

在交换机 C2960-0-3-1 端口 Fa0/2～Fa 0/24 上配置基于 ARP ACL 的 DAI,如下所示。

```
C2960-0-3-1(config)# no  ip dhcp  snooping                                                  ①
C2960-0-3-1(config)# no  ip  dhcp  snooping  vlan  300
C2960-0-3-1(config)# end
C2960-0-3-1# clear  ip  dhcp  snooping  binding  *                                          ②
C2960-0-3-1(config)# arp  access-list  testarp                                              ③
C2960-0-3-1(config-arp-nacl)# permit  ip  host  200.100.10.6  mac  host  PCb 的 MAC         ④
C2960-0-3-1(config-arp-nacl)# permit  ip  host  200.100.10.4  mac  host  PCa 的 MAC         ⑤
C2960-0-3-1(config-arp-nacl)# permit  ip  host  200.100.10.3  mac  host  PCc 的 MAC         ⑥
C2960-0-3-1(config-arp-nacl)# exit
C2960-0-3-1(config)# ip  arp  inspection  filter  testarp  vlan  300                        ⑦
C2960-0-3-1(config)# ip  arp  inspection  vlan  300                                         ⑧
C2960-0-3-1(config)# exit
C2960-0-3-1# show  ip  arp  inspection  vlan  300                                           ⑨

Source Mac Validation        : Disabled
Destination Mac Validation   : Disabled
IP Address Validation        : Disabled

Vlan    Configuration    Operation    ACL Match         Static ACL
----    -------------    ---------    ---------         ---------
300     Enabled          Active       testarp           Yes

Vlan    ACL Logging      DHCP Logging       Probe Logging
----    -----------      ------------       -------------
300     Deny             Deny               Off
 * Mar  1 03:56:06.848: %SW_DAI-4-ACL_DENY: 1 Invalid ARPs (Req) on Fa0/9, vlan 300.
([0015.5886.bcec/169.254.104.52/0000.0000.0000/200.100.10.1/03:56:05 UTC Mon Mar 1
1993])                                                                                      ⑩
```

以上配置操作的含义如下。

① 关闭交换机上的 DHCP 监听。

② 清除已有的所有 DHCP 绑定表条目。

③ 创建一个名为 testarp 的 ARP ACL。

④ 配置 PCb 的 IP-MAC 静态绑定信息。

⑤ 配置 PCa 的 IP-MAC 静态绑定信息。

⑥ 配置 PCc 的 IP-MAC 静态绑定信息。

⑦ 将 ARP ACL 应用到 VLAN300 上。

⑧ 在 VLAN300 上启用 DAI。

⑨ 检查 VLAN300 上的 DAI 配置,可以看到 VLAN300 上使用 Static ACL,ACL 名为 testarp。

⑩ 在 PCc 上发动 ARP 攻击,此时在被攻击主机上启用 Wireshark,应检测不到 ARP 请求报文,交换机报 ARP 请求报文错误。

配置完成后运行 DAI 检查命令,检查配置情况,并在 PCc 上运行 ARP 攻击软件,测

试配置是否起到作用。

7. 实训报告

网络连接配置

主机	IP 地址	掩码	MAC 地址
PCc			
DHCP 服务器			

(1) 用 PCc 假冒 DHCP 服务器，在 PCa、PCb 上运行 Wireshark 监听 bootp 协议报文，并使用 ipconfig/renew 命令重新获得 IP。

主机	IP 地址	掩码	网关 IP	DHCP 服务器 MAC 地址
PCa				
PCb				

(2) 交换机启用 DHCP 监听后，在 PCa、PCb 上运行 Wireshark 监听 bootp 协议报文，并使用 ipconfig/renew 命令重新获得 IP。

主机	IP 地址	掩码	网关 IP	DHCP 服务器 MAC 地址
PCa				
PCb				

(3) 在 PCc 上运行 smurf 攻击 PCa、PCb、网关后，PCa、PCb、网关的网络连接及系统状态。

主机	网络连接和系统状态
PCa	
PCb	
网关	

(4) 在交换机上的静态 IPSG 配置命令。	

继续用 PCc 运行 smurf 攻击 PCa、PCb、网关，PCa、PCb、网关的网络连接及系统状态。

主机	网络连接和系统状态
PCa	
PCb	
网关	

(5) 在 PCc 上运行 ARP 攻击软件攻击 PCa、PCb 后，PCa、PCb 的 ARP 缓存情况。

主机	ARP 缓存中网关、PCa、PCb 的 MAC
PCa	
PCb	

(6) 在交换机上配置基于 DHCP 监听的 DAI 后，PCa、PCb 的 ARP 缓存情况。

主机	ARP 缓存中网关、PCa、PCb 的 MAC
PCa	
PCb	

(7) 在交换机上配置基于 ARP ACL 的 DAI 后，PCa、PCb 的 ARP 缓存情况。

主机	ARP 缓存中网关、PCa、PCb 的 MAC
PCa	
PCb	

第 4 章

网络地址转换技术

本章任务： 根据工程任务安全需求分析，解决网络中使用路由器进行内外网地址转换的配置问题。

必备知识： (1) NAT。
(2) PAT。
(3) 端口重定向。

学习目标： 完成模拟公司分支机构网络内外网地址转换配置任务，解决公司内网地址资源不足的问题。

4.1 模拟公司分支机构网络地址转换任务分析

由表 2-10 所示模拟公司 IP 地址分配情况可知，分支机构 B-1 可用公共 IP 地址仅有 62 个，但随着该分支机构业务发展，网络不断扩大，所分配公共 IP 地址出现不足。为解决 IP 地址紧张问题，模拟公司分支机构 B-1 网络内准备使用私有地址 10.0.0.0/24 替换原网络中的公共 IP 地址。但使用私有地址的分支机构网络不能与分支机构以外的网络通信，为满足分支机构网络以下通信要求，必须使用地址转换技术对进出分支机构网络的报文进行地址转换。

(1) 分支机构 B-1 内部网络中服务器 Ser1 向外网同时提供 Web、邮件服务，同时 1 台独立的 Web 服务器 WebSer1 和 1 台独立的邮件服务器 MailSer1 也向外网提供服务。

(2) 分支机构 8 名主管的办公用机需要使用访问网络上的多媒体服务。

(3) 分支机构 B-1 内部网络中 200 台主机要能访问 Internet 资源。

(4) 分支机构 B-1 在其网络内部模拟公司总部生产网搭建了一套生产系统。该模拟生产系统在分支机构网络内使用了与总部相同的网络地址 200.100.11.0/24，但该生产系统有时需要访问总部生产网下载部分生产数据用于分析研究。

(5) 尽可能节省公共 IP 地址。

表 4-1 显示了分支机构 B-1 内各主机使用 IP 地址情况。

表 4-1　分支机构 B-1 IP 地址分配情况

序　号	内 网 主 机	内部本地地址/网络前缀	网 关 地 址
1	模拟生产系统	10.0.0.0/28	10.0.0.14
2	Ser1	10.0.0.17/28	10.0.0.30
3	WebSer1	10.0.0.18/28	10.0.0.30
4	MailSer1	10.0.0.19/28	10.0.0.30
5	普通主机	10.0.2.0/24	10.0.2.254
6	主管用机	10.0.3.0/24	10.0.3.254

4.2　网络地址转换简介

使用私有地址是目前解决 IPv4 地址不足问题的主要手段。如图 4-1 所示，企业可在各自网络内使用私有地址满足网络内主机间通信需求，不需占用公共 IP 地址资源。

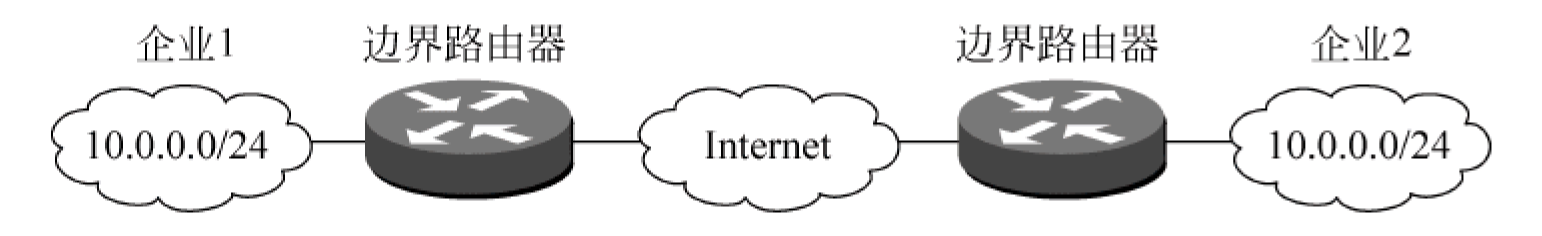


图 4-1　重叠使用的私有地址

IETF RFC 1918 标准定义了 3 段可以重叠使用的私有地址空间，其范围如表 4-2 所示。

表 4-2　私有地址范围

类	地 址 范 围
A	10.0.0.0～10.255.255.255
B	172.16.0.0～172.31.255.255
C	192.168.0.0～192.168.255.255

当企业网络内主机与其他网络通信时，重叠使用的私有地址无法标识通信主机所在网络，所以要实现网络间通信，必须在数据报文被送出本地网络前，将报文中的私有地址转换为公共 IP 地址，即进行地址转换。

4.2.1　地址转换工作过程

地址转换一般在网络边界由网络地址转换设备执行，如配置了地址转换功能的路由器或防火墙。地址转换设备使用"地址转换表"保存地址映射关系记录，并根据地址转换表中的地址映射关系条目对地址进行转换。

图 4-2 显示了一次典型的网络地址转换过程。企业内部网络中的主机 PCa 使用地址 10.0.0.200 向外部网络的主机 PCb 发出数据报文。当这些报文在网络边界碰到网络地址转换设备时，网络地址转换设备根据地址转换表中的地址映射关系，将数据报文中 PCa 的在内部网络中使用的地址 10.0.0.200 转换为公共 IP 地址 200.100.10.200。而 PCb 返回数据报文给 200.100.10.200 时，这些报文也会被网络地址转换设备根据地址转换表进行反向地址转换，即将报文中 PCa 的地址 200.100.10.200 转换为 10.0.0.200。

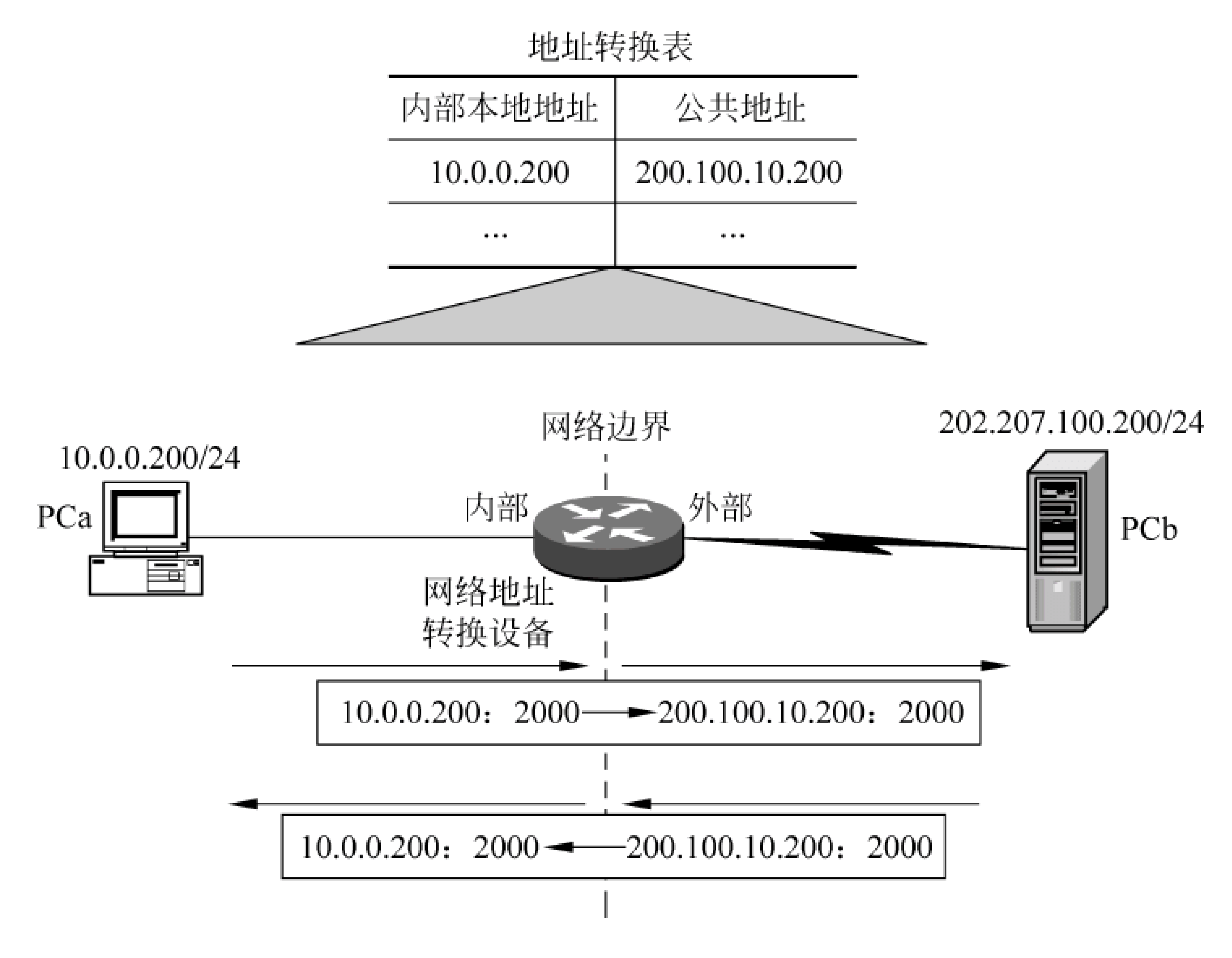


图 4-2　NAT 处理过程示意图

4.2.2　网络地址转换类型及术语

从不同角度出发，可将网络地址转换分为多种类型。表 4-3 显示了各种类型的网络地址转换的含义。

表 4-3　网络地址转换类型

分　类	网络地址转换类型	说　　明
地址转换对象	内部地址转换(NAT Inside)	对本地网络内主机使用的地址进行转换 这种地址转换用于将本地网络内主机使用的私有地址转换为公共网络中能够使用的公共地址
	外部地址转换(NAT Outside)	对外部网络主机地址进行转换 这种地址转换用于当外部网络主机使用的公共地址与本地网络内主机地址相同时，将外部网络主机的公共地址转换为本地网络内可以标识的本地网络地址
地址映射关系	网络地址转换(Network Address Translation，NAT)	将一个 IP 地址转换为另一个 IP 地址
	端口地址转换(Port Address Translation，PAT)	将多个 IP 地址转换为一个 IP 地址，也称为地址重载
地址映射关系形成方式	静态地址转换(Static)	手工定义地址映射关系
	动态地址转换	根据规则动态生成地址映射关系

网络地址转换过程中，在本地网络内部使用的地址被称为“本地地址”(local)，在公共网络中使用的地址被称为“全局地址”(global)。

实际使用的网络地址转换类型一般是以上几种 NAT 转换的组合。表 4-4 显示了各

种常用组合地址转换类型及其适用对象。

表 4-4　各种常见地址转换类型

地址转换类型	说　　明
内部静态 NAT	根据手工配置定义，将内部 IP 地址一对一转换为公共 IP 地址。适用于需要固定 IP 和端口的内网服务器
内部动态 NAT	将一个内部 IP 地址动态转换为一个公共 IP 地址。但所用公共 IP 地址是从指定地址池(Pool)中选取当前可用的最小 IP 地址。地址转换映射关系不会固定存在。适用于不需要固定 IP 和端口的内网主机
内部动态 PAT	将多个内部 IP 地址动态转换为一个公共 IP 地址。公共地址可以是一个 IP 地址，也可以从指定地址池中动态选择当前可用的最小 IP 地址。适用于不需要固定 IP 和端口的内网主机
内部端口地址重定向	手工指定将一个内部 IP 地址和内部端口转换为某个公共 IP 地址及某个公共地址端口。适用于使用一个公共 IP 地址对外提供网络服务的内网多台服务器以及其他需要指定端口映射关系的情况
外部静态 NAT	根据手工配置地址映射关系定义，将某个外网公共 IP 地址一对一转换为本地 IP 地址。适用于重叠地址外网中的服务器
外部动态 NAT	将某外网公共 IP 地址动态转换为本地 IP 地址。但本地 IP 地址从指定地址池中动态选取当前可用最小 IP 地址，地址映射关系不会固定存在。适用于重叠地址外网中的主机
外部静态 PAT	手工指定将一个外部网络 IP 地址和外部端口转换为某个本地网络 IP 地址及某个本地网络地址端口。适用于重叠地址外网中共用一个 IP 地址的多个服务器

1. PAT 工作原理

在网络边界上一对一进行 IP 地址转换，需要较多的公共 IP 地址资源。例如，如果企业内部网络对外连接并发地址数需求为 16，即同时会有 16 个内部 IP 地址访问外部网络，则该企业就需要拥有 16 个以上的公共 IP 地址来满足通信需求。

与 NAT 相比，PAT 技术可以将多个内部网络的私有 IP 地址映射到一个或多个公共 IP 地址上，来减少对公共 IP 地址的需求。图 4-3 为典型 PAT 工作过程示意图，多个内部网络的本地地址被转换为一个公共 IP 地址。进行地址转换时，一般网络地址转换设备会尽量使用与本地地址端口相同的全局地址端口，但如果相同的端口已被占用，则会选择最小的可用端口作为全局地址端口。

地址转换表

内部本地地址	内部本地地址端口	内部全局地址	内部全局地址端口
10.0.0.200	2000	200.100.10.200	2000
10.0.0.100	1024		1024
10.0.0.101	1024		1025
…	…		…

图 4-3　PAT 转换示意图

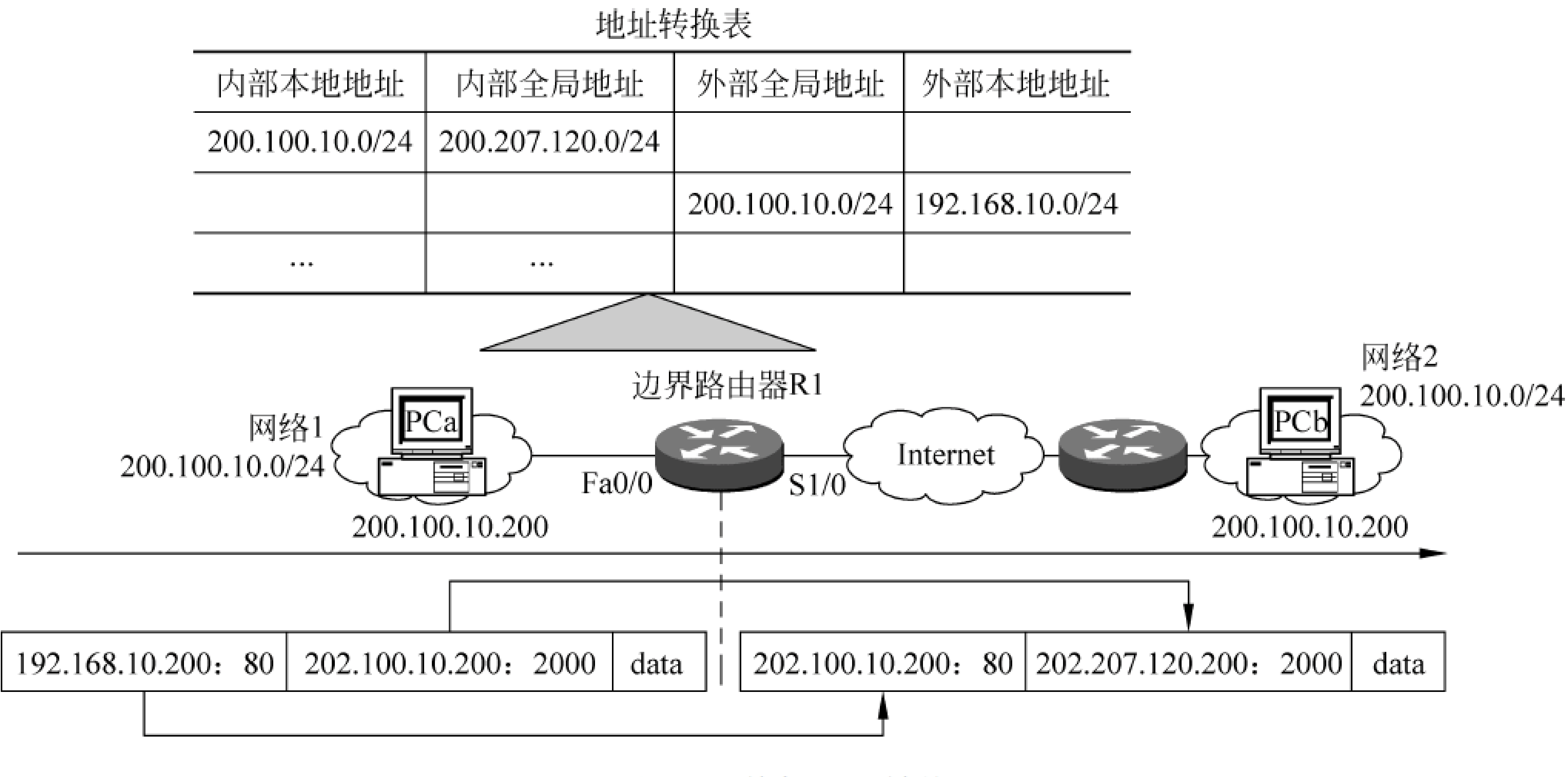
理论上，每个公共 IP 地址可以提供 65536 个端口用于 PAT，但由于有些端口被保留不能使用，所以实际一个公共 IP 仅能提供 4000 个左右主机使用 PAT。

由于使用 PAT 不能保证全局地址端口与原地址端口相同，所以对于需要固定地址端口的服务器而言，如果要使用 PAT，就必须手工指定其地址转换中原端口与全局端口间的映射关系，即端口重定向。

2. 外部地址转换

外部地址转换用于图 4-4 所示网络连接情况。出于某些原因，网络 1 在内部使用了与网络 2 相同的网络地址 200.100.10.0/24，虽然网络 1 在外部使用了公共网络地址 202.207.120.0/24，但如果直接将网络 1 与网络 2 连接起来，网络 1 端的主机将无法区分通信对象属于本网络，还是属于网络 2。在不能通过重新规划 IP 地址解决该问题的时候，外部地址转换就可以作为解决该问题的替代方案。

外部地址转换的工作过程如图 4-4 所示，通过在边界路由器 R1 上将数据报文中网络 2 的主机地址变换成另一个网络 192.168.10.0/24 中的地址，使得网络 1 主机可以使用 192.168.10.0/24 的地址访问网络 2 内的主机。


地址转换表

内部本地地址	内部全局地址	外部全局地址	外部本地地址
200.100.10.0/24	200.207.120.0/24		
		200.100.10.0/24	192.168.10.0/24
…	…		

图 4-4　外部地址转换

注意：在此地址转换过程中，相对于边界路由器 R1 的本地网络，网络 2 主机使用的地址 200.100.10.0/24 是公共 IP 地址，并且是外部网络的地址，所以被称为“外部全局地址”(Outside Global Address)；而由边界路由器转换后的地址 192.168.10.0/24 由于在本地使用，所以被称为“外部本地地址”(Outside Local Address)。

4.2.3　地址转换与访问控制

图 4-5 显示了路由器进行访问控制、地址转换和路由处理的先后顺序。

当数据报文从路由器的内部接口入站，然后从外部接口出站时，路由器处理顺序如下。

(1) 对入站报文进行入站访问控制处理。

(2) 为通过入站访问控制的报文选择合适的路由。

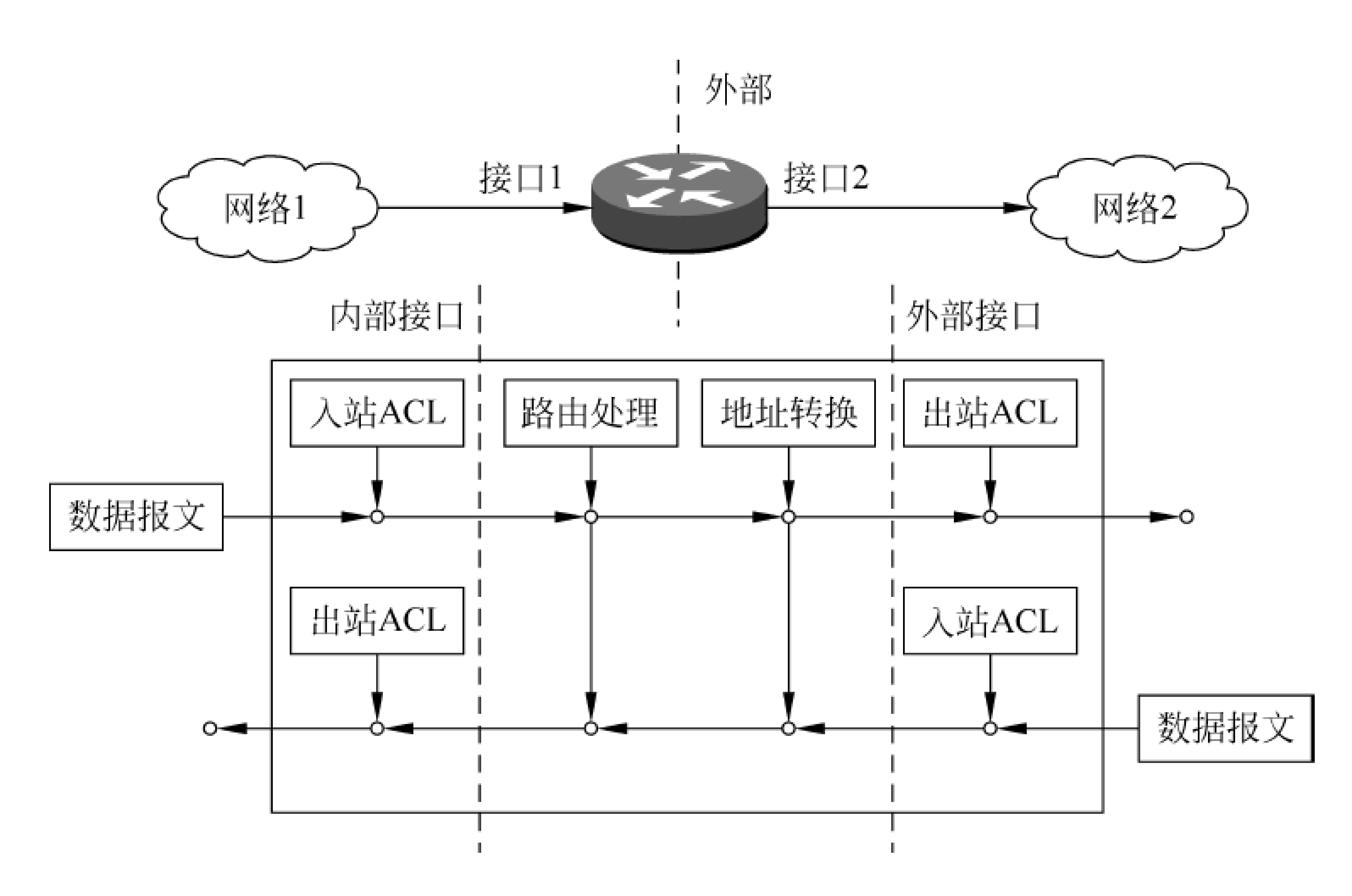


图 4-5　访问控制、地址转换及路由顺序

（3）对于被路由到路由器外部接口的报文，在将其从外部接口送出前，先对数据报文进行地址转换。

（4）转换地址后的数据报文，只有通过出站访问控制处理后，才能真正被送出外部接口。

当数据报文从路由器的外部接口入站，然后从内部接口出站时，路由器处理顺序如下。

（1）对入站报文进行入站访问控制处理。

（2）对通过入站访问控制的报文进行地址转换。

（3）为地址转换后的数据报文选择合适的路由。

（4）对路由到内部接口的数据报文进行出站访问控制处理。

4.2.4　网络地址转换存在的问题

网络设备在进行网络地址转换时，一般只对 IP、TCP、UDP 报头中的 IP 地址、端口进行修改，所以对以下协议报文进行网络地址转换时会出现问题。

（1）如果应用协议在报文中嵌入了 IP 地址和端口号等信息，但网络地址转换设备无法将这些 IP 地址、端口号一并进行转换，则有可能导致相关应用工作失败。

例如，DNS 响应信息、DNS 区域记录中有可能会包含某个域名对应的私有 IP 地址，由于网络地址转换一般不会对这些信息进行转换，所以得到该 DNS 响应信息的主机将不能利用其中的 IP 地址进行通信。类似的还有路由选择更新、IGMP 组播消息、DHCP 报文、BOOTP 报文、NetBIOS 应用报文、一些多媒体应用报文、SQL 服务器连接等。

（2）地址转换不能对加密过的报文头或报文进行，例如 IPSec VPN。

（3）ICMP 报文中没有端口号，因此需要使用 ICMP 报文中的其他信息来区分 PAT 会话连接。但因为使用哪些信息来区分 PAT 还没有相应标准和协议定义，所以不能保证在不同品牌网络设备在配置了 PAT 后，能够正常使用 ICMP。

（4）有些网络地址转换设备不支持对组播地址进行地址转换。

Cisco 网络设备能对某些协议报文中嵌入的 IP 地址、端口号进行地址转换，这被称为应用层网关地址转换支持。但并不是所有嵌入 IP 地址、端口号的应用协议报文都能得到网络设备地址转换支持。

4.3 路由器网络地址转换配置

4.3.1 静态 NAT 配置

如果某网络使用私有地址，但网络中的服务器又要对外提供网络服务，则最简单的实现方法就是为这些服务器配置静态内部 NAT 转换。

在 Cisco IOS 路由器上配置静态 NAT 转换的操作步骤如表 4-5 所示。首先，定义内部地址转换的映射关系，即定义将内网服务器 IP 地址转换为哪个公共地址；然后，定义路由器哪些接口连接内部网络，哪些接口连接外部网络，路由器只在定义为内部或外部的接口进行地址转换；最后，可以对地址转换进行检查，确保配置正确性。

表 4-5 NAT 转换基本配置步骤

序号	操作	相关命令	是否必要
步骤 1	定义地址转换映射关系	**ip nat**	必要
步骤 2	定义路由器地址转换的内部接口	**ip nat inside**	必要
步骤 3	定义路由器地址转换的外部接口	**ip nat outside**	必要
步骤 4	检查地址转换配置	**show ip nat translations** **debug ip nat** **clear ip nat translation**	可选

1. 定义内部地址转换映射关系

在 Cisco IOS 路由器上，定义一对一内部地址转换映射关系的操作为在全局模式下输入：

ip nat inside source static 内部本地地址 {内部全局地址 | **interface** 接口号}

该命令用于配置一个内部地址转换，将参数“内部本地地址”指定的本地地址转换为参数“内部全局地址”指定的公共地址或参数“接口号”指定的某个接口的地址。

关键字 source 表示要对报文中的源地址进行转换。

关键字 static 表示地址转换是一对一的静态地址转换。

例如，若图 4-2 中 PCa 为内网服务器，其内网地址为 10.0.0.200，现要从公网使用 IP 地址 200.100.10.200 访问该服务器，则定义这一地址转换映射关系的命令为：

Router(config)# **ip nat inside source static 10.0.0.200 200.100.10.200**

另外，如果一个网络内存在多台服务器需要进行一对一地址转换，则可以将这些服务器尽可能安排一个网络内，然后在 Cisco IOS 路由器上使用如下命令。

ip　nat　inside　source　static　network 内部本地网络地址　内部全局网络地址　{ 网络前缀　| 子网掩码 }

该命令可以将一个网络的 IP 地址一对一转换为另一个网络的 IP 地址。

例如,如果要将网络 10.0.0.0/24 中所有 IP 地址一对一转换为 200.100.10.0/24,则可以如下定义地址映射关系。

Router(config)# **ip　nat　inside　source　static　network　10.0.0.0　200.100.10.0　/24**

路由器根据该命令进行地址转换时,将只改变本地地址的网络号部分,本地地址 10.0.0.2 转换后为 200.100.10.2,本地地址 10.0.0.11 转换后为 200.100.10.11。

2. 定义路由器地址转换的内部、外部接口

要让路由器能正确进行地址转换,还需定义路由器哪些接口连接地址转换的内部网络,哪些接口连接地址转换的外部网络。

配置接口是连接内部网络的操作为在该接口配置模式下输入:

ip　nat　inside

配置接口是连接外部网络的操作为在该接口配置模式下输入:

ip　nat　outside

3. 检查地址转换配置

(1) 使用 show　ip　nat　translations 命令检查地址转换配置

在 Cisco IOS 路由器上,可以使用 show　ip　nat　translations 命令来检查地址转换配置,该命令输出结果如下。

```
Router1# show  ip  nat  translations
Pro   Inside global      Inside local      Outside local      Outside global
---   200.100.10.200     10.0.0.200        ---                ---
```

该输出结果显示"地址转换表"中保存了一条内部地址转换映射信息,从内部本地地址 10.0.0.200 转换为内部全局地址 200.100.10.200。

(2) 使用 debug　ip　nat 命令跟踪地址转换

在 Cisco IOS 路由器上,也可以使用 debug　ip　nat 命令来打开对地址转换的跟踪显示。在打开地址转换跟踪显示后,只要有地址转换发生,路由器屏幕上就会显示地址转换过程的详细信息,打开地址转换跟踪显示配置的操作及路由器跟踪到的地址转换过程信息如下。

```
Router1# debug  ip  nat
IP NAT debugging is on
Router1#
*Mar  1 00:15:37.747: NAT*: i: icmp (10.0.0.200, 3286) -> (200.100.0.1, 3286) [38]   ①
*Mar  1 00:15:37.747: NAT*: s=10.0.0.200->200.100.10.200, d=200.100.0.1 [38]   ②
*Mar  1 00:15:37.887: NAT*: o: icmp (200.100.0.1, 3286) -> (200.100.10.200, 3286) [38]   ③
*Mar  1 00:15:37.887: NAT*: s=200.100.0.1, d=200.100.10.200->10.0.0.200 [38]   ④
```

其中：

① 内网主机 10.0.0.200 向外网主机 200.100.0.1 发送 ICMP ECHO 报文。

② 路由器将内网主机报文中源地址 10.0.0.200 转换为公共地址 200.100.10.200。

③ 外网主机 200.100.0.1 返回 ICMP 报文给内网主机 200.100.10.200。

④ 路由器将外网 ICMP 返回报文中的目的地址 200.100.10.200 转换为内网地址 10.0.0.200。

4. 清除地址转换表缓存

在检查地址转换配置过程中，可以先使用如下命令来清除路由器“地址转换表”中缓存的地址映射关系条目。

```
clear ip nat translation *
```

或者

```
clear ip nat translation { inside | outside }
```

使用“*”关键字，将清除所有地址转换表中动态映射关系条目，使用 inside 或 outside 关键字，则可以选择性地只清除某个方向的地址转换条目。

4.3.2 动态 NAT 配置

企业内网主机由于不需要对外提供网络服务，因而不需要固定的公共 IP 和端口地址，所以可以选用动态 NAT 转换或者动态 PAT 作为地址转换类型。

在 Cisco IOS 路由器上配置动态 NAT 的操作步骤如表 4-6 所示。相对静态 NAT 转换，动态 NAT 转换增加了两个用于定义地址转换范围的步骤：①使用 ip nat pool 命令定义一个用于地址转换的地址池；②使用 ip access-list 或者 access-list 命令定义一个访问控制列表，只有该列表中允许的流量才会被进行地址转换。

另外，定义动态 NAT 地址转换映射关系条目的命令语法与静态 NAT 不同。

表 4-6 动态 NAT 转换基本配置步骤

序 号	操 作	相关命令	是否必要
步骤 1	定义地址池	**ip nat pool**	必要
步骤 2	创建一个用于限制被转换地址范围的 ACL	**ip access-list**、**access-list**	必要
步骤 3	定义地址转换映射关系条目	**ip nat**	必要
步骤 4	定义路由器地址转换的内部接口	**ip nat inside**	必要
步骤 5	定义路由器地址转换的外部接口	**ip nat outside**	必要
步骤 6	检查地址转换配置	**show ip nat translations** **debug ip nat**	可选

1. 定义地址池

在 Cisco IOS 路由器上，定义地址池的操作为在全局模式下输入：

ip nat pool 地址池名 起始 IP 地址 结束 IP 地址 { **netmask** 子网掩码 | **prefix-length** 网络前缀长度 }

参数“地址池名”用于给出该地址池的唯一标识。

参数“起始 IP 地址”、“结束 IP 地址”用于定义地址池中 IP 地址的起止范围。

关键字 netmask、prefix-length 及其后参数用于给出起止 IP 地址所在网络的子网掩码或网络前缀。

例如，若企业租用的公共 IP 地址范围为 200.100.10.0～200.100.10.15，子网掩码为 255.255.255.240，则可如下定义地址池。

```
Router1(config)# ip nat pool natdp-in 200.100.10.0 200.100.10.15 netmask  255.255.255.240
```

该命令创建一个名为 natdp-in 的地址池，该地址池地址范围为 200.100.10.0～200.100.10.15，此段地址所在网络的子网掩码为 255.255.255.240。

2. 定义内部动态 NAT 地址映射关系条目

在 Cisco IOS 路由器上定义内部动态 NAT 地址映射关系的操作为在全局模式下输入：

```
ip  nat  inside  source  list  ACL 名  pool  全局地址池名
```

该命令中，参数“ACL 名”将指定一个标准访问控制列表，只有被该标准访问控制列表允许的流量，才会被进行内部动态 NAT 处理。

参数“全局地址池名”用于将前面定义的全局地址池与该地址映射绑定在一起。

例如，图 4-6 所示为企业内部网络使用的 IP 地址为 10.0.0.0/24，企业租用的公共 IP 地址范围是 200.100.10.0～200.100.10.15，则在边界路由器上配置动态 NAT 的操作如下。

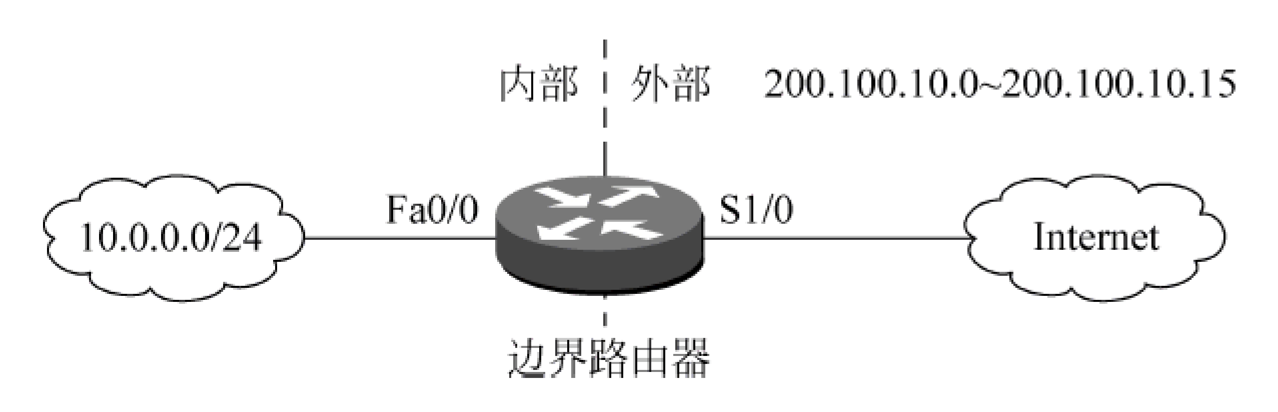


图 4-6　动态 NAT 网络

```
Router1(config)# ip  nat  pool  p-natin  200.100.10.0  200.100.10.15  netmask  255.255.255.240
Router1(config)# ip  access-list  standard  sacl-dnatin
Router1 (config-std-nacl)# permit  10.0.0.0  0.0.0.255
Router1 (config-std-nacl)# exit
Router1(config)# ip  nat  inside  source  list  sacl-dnatin  pool  p-natin
Router1(config-if)# interface  fa0/0
Router1(config-if)# ip  nat  inside
Router1(config-if)# interface  s1/0
Router1(config-if)# ip  nat  outside
Router1(config-if)# end
Router1# show  ip  nat  translations
Pro  Inside global    Inside local    Outside local    Outside global
---  200.100.10.1     10.0.0.200      ---              ---
```

4.3.3 动态 PAT 配置

在 Cisco IOS 路由器上配置动态 PAT 的操作步骤与配置动态 NAT 非常相似，如表 4-7 所示。

表 4-7 PAT 基本配置步骤

序 号	操 作	相关命令	是否必要
步骤 1	定义地址池	**ip nat pool**	根据网络实际需求确定
步骤 2	创建一个用于限制被转换地址范围的 ACL	**ip access-list、access-list**	必要
步骤 3	定义地址转换映射关系条目	**ip nat … overload**	必要
步骤 4	定义路由器地址转换的内部接口	**ip nat inside**	必要
步骤 5	定义路由器地址转换的外部接口	**ip nat outside**	必要
步骤 6	检查地址转换配置	**show ip nat translations** **debug ip nat**	可选

动态 PAT 与动态 NAT 在配置操作上的主要区别如下。

定义 PAT 地址映射关系条目时，命令最后要增加一个表示重载的关键字 overload，这是进行 PAT 转换的标志。

另外，配置动态 NAT 时，定义全局地址池是必要的；但定义 PAT 时，却未必。可以根据企业网络规模和网络流量情况，将所有内部地址重载到一个公共地址上，或一个地址池中的多个公共地址上。

在 Cisco IOS 路由器上，定义动态 PAT 地址转换映射关系条目的操作为在全局配置模式下输入：

ip nat inside source list ACL 名 ｛ **pool** 全局地址池名 ｜ **interface** 接口号 ｝ **overload**

1. 重载到多个 IP 地址的 PAT 配置

例如，在图 4-6 中边界路由器上配置 PAT，将内部网络 10.0.0.0/24 中 IP 地址映射到地址池 200.100.10.0～200.100.10.15 上的操作如下。

```
Router1(config)# ip nat pool p-natin 200.100.10.0 200.100.10.15 netmask 255.255.255.240
Router1(config)# ip access-list standard sacl-dnatin
Router1 (config-std-nacl)# permit 10.0.0.0 0.0.0.255
Router1 (config-std-nacl)# exit
Router1(config)# ip nat inside source list sacl-dnatin pool p-natin overload
Router1(config-if)# interface fa0/0
Router1(config-if)# ip nat inside
Router1(config-if)# interface s1/0
Router1(config-if)# ip nat outside
Router1(config-if)# end
Router1# show ip nat translations
Pro   Inside global        Inside local      Outside local         Outside global
icmp  200.100.10.1:7264    10.0.0.2:7264     200.100.10.101:7264   200.100.10.101:7264
```

注意：从 show ip nat translations 命令输出结果可以发现，地址转换表中除了

记录 IP 地址还记录了端口信息。

2. 重载到接口地址的 PAT 配置

为节省地址资源，Cisco IOS 还允许将内部地址转换为某个接口的地址，这种多对一转换也称为地址重载。要配置重载到接口的 PAT，只需在定义地址映射关系条目时，使用关键字 interface，并后跟重载的接口号，然后在最后带上 overload 关键字。

例如，要将 10.0.0.0/24 网络内的地址转换为接口 S1/0 的地址，则可以如下配置。

```
Router1(config)# ip access-list standard sacl-dnatin
Router1 (config-std-nacl)# permit 10.0.0.0 0.0.0.255
Router1 (config-std-nacl)# exit
Router1(config)# ip nat inside source list sacl-dnatin interface s1/0 overload
Router1(config-if)# interface fa0/0
Router1(config-if)# ip nat inside
Router1(config-if)# interface s1/0
Router1(config-if)# ip address 200.100.10.10 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# ip nat outside
Router1(config-if)# end
Router1# show ip nat translations
Pro   Inside global        Inside local      Outside local      Outside global
icmp  200.100.10.10:4885   10.0.0.2:4885     172.16.16.1:4885   172.16.16.1:4885
```

4.3.4 端口地址重定向配置

实际网络中常在以下情况使用端口重定向(Port Address Redirection，PAR)来满足地址转换需求。

(1) 内网服务器要对外网提供服务，但只有 1 个公共地址，该地址又必须配置在边界路由器连接外部网络的接口上。

(2) 公共地址不足以为所有内网服务器配置静态 NAT。

(3) 希望使用与内网服务器不同的端口对外提供网络服务。

在 Cisco IOS 路由器上，定义端口地址重定向的操作步骤与静态 NAT 配置相同，仅在定义地址映射关系条目的命令语法上有所不同。

在 Cisco IOS 路由器上，定义端口地址重定向地址映射关系条目的操作为在全局模式下输入：

ip nat inside source static { tcp | udp } 内部本地地址 内部本地地址端口号 内部全局地址 内部全局地址端口号

例如，若内网 Web 服务器地址为 10.0.0.10，企业租用的公共 IP 地址为 200.100.10.2，则定义相应地址转换映射关系条目的操作为：

```
Router1(config)# ip nat inside source static tcp 10.0.0.10 80 200.100.10.2 80
```

4.3.5 外部地址转换配置

如果内部网络需要访问某地址重叠的外网服务器，可以通过配置静态外部 NAT 转换或静态外部 PAT 转换实现。

如果内部网络同时要访问某地址重叠的外网内主机，则可以通过配置动态外部 NAT 转换实现。

在 Cisco IOS 路由器上，配置静态外部 NAT、动态 NAT 和静态 PAT 的操作步骤与配置内部 NAT、PAT 相同，只是在定义地址映射关系条目时有部分参数不同。

在 Cisco IOS 路由器上，定义静态外部 NAT 地址转换映射关系条目的操作为在全局模式下输入：

ip　nat　outside　source　static 外部全局地址　外部本地地址

注意： 该命令使用 outside 关键字，表明该命令是对外部地址进行转换；另外，被转换的地址是“外部全局地址”，在参数“外部全局地址”位置给出；转换后的地址是“外部本地地址”，在参数“外部本地地址”位置给出。

例如，若图 4-4 中 PCb 为某外部网络服务器，其 IP 地址为 200.100.10.200，与图中网络 1 的网络地址重叠。为使网络 1 中主机能访问该服务器，需在网络 1 边界路由器上为其配置外部地址转换，将其地址在到达网络 1 时转换为 192.168.10.200。定义这一地址转换映射关系的命令为：

Router(config)# **ip　nat　outside　source　static　200.100.10.200　192.168.10.200**

在 Cisco IOS 路由器上，定义动态外部 NAT 地址转换映射关系条目的操作为在全局模式下输入：

ip　nat　outside　source　list 外部全局地址 ACL 名　**pool** 外部本地地址池名

而在 Cisco IOS 路由器上，定义静态外部 PAT 地址转换映射关系条目的操作为在全局模式下输入：

ip　nat　outside　source　static ｛**tcp**｜**udp**｝ 外部全局地址　端口号　外部本地地址　端口号

4.4　模拟公司分支机构地址转换配置方案

分支机构 B-1 需要在网络边界上使用路由器完成地址转换任务。可按表 4-8 所示地址转换方案，配置边界路由器，以满足 4.1 节定义的网络地址转换任务需求。

表 4-8　分支机构网络地址转换情况

内网主机	地址转换类型	内部本地地址	端口	全 局 地 址	全局地址前缀	全局端口	外部本地地址
模拟生产系统	内部静态 NAT	200.100.11.0/28		200.100.15.0～200.100.15.15	26		
总部生产系统	外部静态 NAT			200.100.11.0～200.100.11.255	24		10.0.1.0/24
Ser1	内部静态 NAT	10.0.0.17/28		200.100.15.17	26		
WebSer1	内部端口重定向	10.0.0.18/28	80	200.100.15.18	26	80	
MailSer1	内部端口重定向	10.0.0.19/28	25			25	
	内部端口重定向		110			110	
普通主机	内部动态 PAT	10.0.2.0/24		200.100.15.32～200.100.15.47	26		
主管用机	内部动态 NAT	10.0.3.0/24		200.100.15.48～200.100.15.56	26		

（1）分支机构的模拟生产系统中各主机需要配置静态 NAT 转换，这样总部可以访问这些主机。

（2）总部生产系统地址与模拟生产系统地址重叠，使用外部静态 NAT，将其转换为本地 10.0.3.0/24。

（3）服务器 Ser1 上宿主多种服务，为保证网络服务性能，使用内部静态 NAT 实现对外服务。

（4）服务器 WebSer1、MailSer1 分别提供 Web 服务和邮件服务，其服务端口不冲突，本着节省 IP 地址资源的原则，可以将其转换为一个公共 IP。

（5）内网有 200 台左右普通主机，根据平时历史统计，每台主机对外并发连接平均在 1000 个左右，考虑到一个公共地址可以提供 4000 个左右 PAT，则至少需要 5 个公共 IP 地址，方案设计为其预留 16 个 IP 地址。

（6）主管用机因为要访问网络多媒体资源，所以不能使用 PAT，考虑使用内部动态 NAT。

4.5　小结

将内部网络连接到 Internet 时，需使用地址转换技术进行私有地址与公共 IP 地址间的转换；地址转换技术分为 NAT、PAT，内部地址转换、外部地址转换，静态地址转换、动态地址转换等；在路由器上配置地址转换的基本步骤分两步：①定义地址转换映射条目；②指定接口地址转换类型。

4.6　习题

1．简述各类 NAT 功能，并举例。

2．有哪些情况使用 PAT 时，不一定能得到网络设备的支持？

3．使用 PAT 时，一个公共 IP 地址可以供多少主机使用？

4．当边界路由器上配置了内部静态 NAT 将本地地址 10.0.0.1 转换为 200.100.1.1 时，是否需要在边界路由器上增加一条到达 200.100.1.0/24 的路由？并解释原因。

4.7　实训

1．实训组织

实训学时：300 分钟。

学生分组：2 人/组。

2．实训目的

通过实训，熟练掌握路由器上配置各类地址转换的操作。

3．实训环境

（1）安装有 Windows 系统、网络服务软件（例如 XAMPP）的 PC，每组 3 台。

（2）Cisco 二层交换机，每组 1 台。
（3）Cisco 路由器，每组 2 台。
（4）UTP 交叉电缆，每组 1 条。
（5）UTP 直通电缆，每组 4 条。
（6）Console 电缆，每组 1 条。
注意保持所有的路由器、交换机为出厂配置。

4. 实训准备

在实训前，实验室教师需完成以下准备工作。

- 按照图 4-7 所示连接实训网络。
- 按照表 4-9 所示，在交换机上划分 VLAN。
- 按照表 4-10 所示，配置路由器接口和 PCc 的 IP 地址，并完成网络连通性配置。
- 在 PCa、PCb、PCc 上配置好实训所需 Web、FTP 等网络服务。

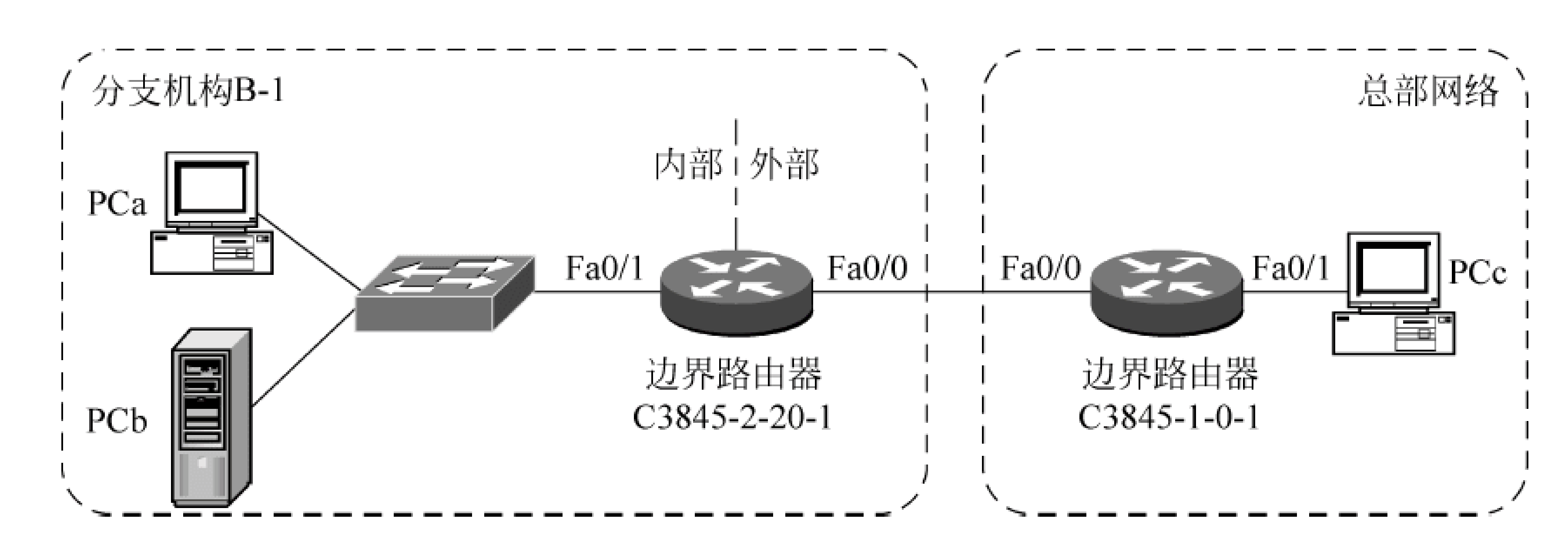


图 4-7 地址转换实训网络拓扑示意图

表 4-9 地址转换实训 VLAN 划分

VLAN 号	说　明	网络地址/前缀
10	分支机构 B-1 模拟生产系统网络	200.100.11.0/28
15	分支机构 B-1 服务器网络	10.0.0.16/28
20	分支机构 B-1 普通主机网络	10.0.2.0/24
30	分支机构 B-1 主管用机网络	10.0.3.0/24

表 4-10 地址转换实训 IP 地址分配

序号	实训项目	接　口	角　色	IP 地址/网络前缀	网　关
	所有项目	C3845-2-20-1 接口 Fa0/0	分支机构外网接口	200.100.15.62/26	
		C3845-2-20-1 接口 Fa0/1.10	分支机构模拟生产系统网关	200.100.11.14	
		C3845-2-20-1 接口 Fa0/1.15	分支机构服务器网关	10.0.0.30	
		C3845-2-20-1 接口 Fa0/1.20	分支机构普通主机网关	10.0.2.254	
		C3845-2-20-1 接口 Fa0/1.30	分支机构主管用机网关	10.0.3.254	
		C3845-1-0-1 接口 Fa0/0	总部外网接口	200.100.15.61/26	
		C3845-1-0-1 接口 Fa0/1	总部内网接口	200.100.11.254/24	
		PCc	总部生产系统主机	200.100.11.1/24	200.100.11.254
1	内部静态 NAT	PCa	分支机构模拟生产系统主机	200.100.11.1/28	200.100.11.14
		PCb	分支机构 Ser1	10.0.0.17/28	10.0.0.30

续表

序号	实训项目	接　口	角　色	IP 地址/网络前缀	网　关
2	内部动态 NAT	PCa	分支机构主管用机	10.0.3.1/24	10.0.3.254
		PCb	分支机构主管用机	10.0.3.2/24	10.0.3.254
3	内部动态 PAT	PCa	分支机构普通用机	10.0.2.1/24	10.0.2.254
		PCb	分支机构普通用机	10.0.2.2/24	10.0.2.254
4	内部端口重定向	PCa	分支机构 WebSer1	10.0.0.18/28	10.0.0.30
		PCb	分支机构 MailSer1	10.0.0.19/28	10.0.0.30
5	外部静态 NAT	PCa	分支机构模拟生产系统主机	200.100.11.1/28	200.100.11.14
		PCb	分支机构模拟生产系统主机	200.100.11.2/28	200.100.11.14

该实训网络拓扑仿照模拟公司分支机构 B-1 网络设计，简化了一些与本次实训内容无关的部分，同时实训中将分支机构 B-1 的邮件服务器 MailSer 改为提供 FTP 服务。

5. 实训内容

(1) 内部静态 NAT 配置。

(2) 内部动态 NAT 配置。

(3) 内部动态 PAT 配置。

(4) 内部端口重定向配置。

(5) 外部静态 NAT 配置。

6. 实训指导

(1) 内部静态 NAT 配置

根据 4.4 节模拟公司分支机构地址转换配置方案中有关描述可知，对于分支机构 B-1，需要进行以下两项静态 NAT 配置。

① 将模拟生产系统中所有主机 IP 200.100.11.0/28 使用静态 NAT 转换为 200.100.15.0～200.100.15.15，这可以通过一个网络到另一个网络的静态 NAT 转换实现。

② 将服务器 Ser1 使用的地址 10.0.0.17 使用静态 NAT 转换为 200.100.15.17，这可以通过一对一的静态 NAT 实现。

在路由器 C3845-2-20-1 实现以上静态 NAT 转换的配置操作如下。

```
C3845-2-20-1(config)# ip nat inside source static network 200.100.11.0 200.100.15.0/28
C3845-2-20-1(config)# ip nat inside source static 10.0.0.17 200.100.15.17
C3845-2-20-1(config)# interface fa0/0
C3845-2-20-1(config-if)# ip nat outside
C3845-2-20-1(config-if)# interface fa0/1.10
C3845-2-20-1(config-subif)# ip nat inside
C3845-2-20-1(config-if)# interface fa0/1.15
C3845-2-20-1(config-subif)# ip nat inside
C3845-2-20-1(config-subif)# end
```

以上配置完成后，使用如下命令，打开地址转换跟踪显示。

```
C3845-2-20-1# debug ip nat
```

按照表 4-10 为 PCa、PCb 配置 IP，然后分别使用 ping 测试从 PCa、PCb 到达 PCc 的

连通性。注意，由于此时 PCa 地址 200.100.11.1 与外部网络 PCc 的地址 200.100.11.1 有重叠，所以 PCa、PCb 此时 ping 不通 PCc。

输入如下命令，检查地址转换配置是否正确。

```
C3845-2-20-1#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 200.100.15.17      10.0.0.17         ---                ---

Subnet translation:
Inside global      Inside local      Outside local    Outside global /prefix
200.100.15.0       200.100.11.0      ---              ---             /28
```

由以上输出结果可以发现，地址转换关系定义是符合地址转换方案要求的。

(2) 内部动态 NAT 配置

根据 4.4 节模拟公司分支机构地址转换配置方案中有关描述可知，对于分支机构 B-1，需要对主管用机 10.0.3.0/24 使用动态 NAT 转换为公共 IP 地址 200.100.15.48～200.100.15.56。相应配置操作如下所示。

```
C3845-2-20-1(config)#ip access-list standard sacl-dnat-lead
C3845-2-20-1(config-std-nacl)#permit 10.0.3.0 0.0.0.255
C3845-2-20-1(config-std-nacl)#exit
C3845-2-20-1(config)#ip nat pool dp-lead 200.100.15.48 200.100.15.56 netmask 255.255.255.192
C3845-2-20-1(config)#ip nat inside source list sacl-dnat-lead pool dp-lead
C3845-2-20-1(config-if)#interface fa0/1.30
C3845-2-20-1(config-subif)#ip nat inside
C3845-2-20-1(config)#end
```

以上配置定义了地址池 dp-lead 和 ACL sacl-dnat-lead。在地址池中，起止地址分别为 200.100.15.48、200.100.15.56，共 8 个 IP，子网掩码为分支机构网络公共 IP 地址的子网掩码 255.255.255.192。

注意：此处如果使用子网掩码 255.255.255.240，则将从 200.100.15.49 开始地址转换。由于分支机构 B-1 网络内没有使用此段公共 IP 地址，所以不用担心此处使用子网掩码 255.255.255.192 会影响路由。

按照表 4-10 修改 PCa、PCb 的 IP 地址，并分别使用 ping 测试 PCa、PCb 到 PCc 的连通性。此时由于已经打开了路由器的地址转换跟踪显示，路由器上会显示如下一些信息。

```
*Mar  1 07:28:16.338: NAT: s=10.0.3.1->200.100.15.48, d=200.100.11.1 [50]
*Mar  1 07:28:16.586: NAT*: s=200.100.11.1, d=200.100.15.48->10.0.3.1 [50]
```

注意：只在需要进行地址转换时，路由器才会建立动态的地址转换信息并保存到地址转换表中，所以当没有匹配的数据报文通过路由器时，使用 show ip nat translations 命令检查动态地址转换，是看不到任何效果的。

(3) 内部动态 PAT 配置

根据 4.4 节模拟公司分支机构地址转换配置方案中有关描述可知，对于分支机构 B-1，需要对分支机构内普通主机 10.0.2.0/24 使用动态 PAT 转换为公共 IP 地址

200.100.15.32～200.100.15.47，相应配置及检查操作如下所示。

```
C3845-2-20-1(config)#ip access-list standard sacl-dpat-pc
C3845-2-20-1(config-std-nacl)#permit 10.0.2.0 0.0.0.255
C3845-2-20-1(config-std-nacl)#exit
C3845-2-20-1(config)#ip nat pool dp-pc 200.100.15.32 200.100.15.47 netmask 255.255.255.192
C3845-2-20-1(config)#ip nat inside source list sacl-dpat-pc pool dp-pc overload
C3845-2-20-1(config-if)#interface fa0/1.20
C3845-2-20-1(config-subif)#ip nat inside
C3845-2-20-1(config)#end
```

按照表 4-10 修改 PCa、PCb 的 IP 地址，然后使用 ping 分别测试 PCa、PCb 到达 PCc 的连通性。测试时，不要忘记在路由器上输入如下命令，检查地址转换表中的动态 PAT 映射信息。

```
C3845-2-20-1#show ip nat translations
Pro Inside global          Inside local       Outside local        Outside global
icmp 200.100.15.34:752     10.0.2.1:752       200.100.11.1:752     200.100.11.1:752
icmp 200.100.15.34:753     10.0.2.1:753       200.100.11.1:753     200.100.11.1:753
icmp 200.100.15.34:754     10.0.2.1:754       200.100.11.1:754     200.100.11.1:754
icmp 200.100.15.34:755     10.0.2.1:755       200.100.11.1:755     200.100.11.1:755
icmp 200.100.15.34:756     10.0.2.1:756       200.100.11.1:756     200.100.11.1:756
--- 200.100.15.17          10.0.0.17          ---                  ---

Subnet translation:
Inside global      Inside local      Outside local     Outside global /prefix
200.100.15.0       200.100.11.0      ---               ---              /28
```

（4）内部端口重定向配置

根据 4.4 节模拟公司分支机构地址转换配置方案中有关描述可知，对于分支机构 B-1，需要将服务器 WebSer1、MailSer1 的地址和端口 10.0.0.18:80、10.0.0.19:21、10.0.0.19:20 使用端口重定向转换到公共 IP 地址 200.100.15.18:80、200.100.15.18:21、200.100.15.18:20，其相应配置如下所示。

```
C3845-2-20-1(config)#ip nat inside source static tcp 10.0.0.18 80 200.100.15.18 80
C3845-2-20-1(config)#ip nat inside source static tcp 10.0.0.19 20 200.100.15.18 20
C3845-2-20-1(config)#ip nat inside source static tcp 10.0.0.19 21 200.100.15.18 21
C3845-2-20-1(config)#end
```

完成以上配置后，按照表 4-10 为 PCa、PCb 配置 IP 地址，然后在 PCc 上使用客户端访问 PCa、PCb 上的 Web 服务、FTP 服务，测试地址转换配置是否能正确转换地址。注意在测试时，使用 show 命令检查地址转换表。例如，当在 PCc 上运行浏览器访问 PCa 上的 Web 服务时，show ip nat translations 命令输出结果可能如下所示。

```
C3845-2-20-1#show ip nat translations
Pro Inside global        Inside local      Outside local         Outside global
tcp 200.100.15.18:80     10.0.0.18:80      200.100.11.1:11000    200.100.11.1:11000
--- 200.100.15.17        10.0.0.17         ---                   ---
tcp 200.100.15.18:20     10.0.0.19:20      ---                   ---
```

```
tcp 200.100.15.18:21    10.0.0.19:21    ---    ---
tcp 200.100.15.18:80    10.0.0.18:80    ---    ---

Subnet translation:
Inside global   Inside local    Outside local   Outside global /prefix
200.100.15.0    200.100.11.0    ---             ---            /28
```

(5) 外部静态 NAT 配置

根据 4.4 节模拟公司分支机构地址转换配置方案中有关描述可知，对于分支机构 B-1，需要对总部生产系统网络进行外部静态 NAT 配置，相应配置如下所示。

```
C3845-1-20-1(config)# ip nat outside source static network 200.100.11.0 10.0.1.0 /24
C3845-2-20-1(config)# end
```

完成以上地址转换配置后，按照表 4-10 为 PCa、PCb 配置 IP 地址，然后使用 ping 分别从 PCa、PCb 上测试到 PCc 的连通性。由于前面配置中打开了地址转换跟踪，所以可能出现如下所示地址转换信息。

```
* Mar  1 11:25:47.433: NAT* : s=200.100.11.1->200.100.15.1, d=10.0.1.254 [223]
* Mar  1 11:25:47.433: NAT* : s=200.100.15.1, d=10.0.1.254->200.100.11.254 [223]
* Mar  1 11:25:47.557: NAT* : s=200.100.11.254->10.0.1.254, d=200.100.15.1 [223]
* Mar  1 11:25:47.557: NAT* : s=10.0.1.254, d=200.100.15.1->200.100.11.1 [223]
```

7. 实训报告

1. 在使用“ip nat inside source static network 200.100.11.0 200.100.15.0/28”命令配置内部静态 NAT 后：

(1) 内部本地地址 200.100.11.3 会被转换为：200.100.15.________________。

(2) 内部地址 200.100.11.254 会被转换为：____________________________。

为什么？答：____。

2. 在配置内部动态 NAT 时，如果使用以下 ACL 定义将被转换的地址，则下列说法正确的是(　　)。

```
ip access-list standard sacl-dnat-lead
 deny host 10.0.3.1
 permit 10.0.3.0 0.0.0.255
 deny host 10.0.3.254
```

A. 内部本地地址 10.0.3.1 将被进行地址转换

B. 内部本地地址 10.0.3.254 不会被进行地址转换

C. 内部本地地址 10.0.3.1 和 10.0.3.254 将被进行地址转换

D. 除 10.0.3.1 和 10.0.3.254 外，网络 10.0.3.0/24 内的所有地址都会被转换

3. 简述配置内部动态 NAT 的步骤。

续表

4. 如果内部动态 PAT 的地址池如下定义，则第一个能被使用的公共 IP 地址是：________。最后一个能被使用的公共 IP 地址是：________。 ip nat pool dp-lead 200.100.15.10　200.100.15.63　netmask 255.255.255.192
5. 在配置内部动态 PAT 后，被用于转换的第一个全局端口是：________。
6. 如果分支机构 B-1 内有多台 Web 服务器要对外提供服务，且全局端口均为 80，那么这些 Web 服务器可以共享 1 个全局 IP 地址吗？　□可以　□不可以
7. 在完成实训中以下外部地址转换配置后： ip　nat　inside　source　static　network　200.100.11.0　200.100.15.0/28 ip　nat　outside　source　static　network　200.100.11.0 10.0.1.0 /24 (1) 从 PCa 上使用 ping 测试到达 PCc 的连通性时，应在 PCa 上输入：ping ________。 (2) 从 PCc 上使用 ping 测试到达 PCa 的连通性时，应在 PCc 上输入：ping ________。

第 5 章

VPN　技　术

本章任务：根据工程任务安全需求分析，解决利用 Internet 线路进行安全通信配置问题。

必备知识：(1) VPN 概念。

(2) 站到站 VPN 配置。

(3) 远程访问 VPN 配置。

学习目标：完成在路由器上创建模拟分公司与分支机构间、分支机构与员工计算机间 VPN 连接的配置任务，保护基于 Internet 线路的网络通信安全。

5.1　模拟公司网络安全通信配置任务分析

如图 5-1 所示，模拟分公司 1 与分支机构 B-1 间租用 Internet 线路进行通信。为保证公司网络通信安全，要求：

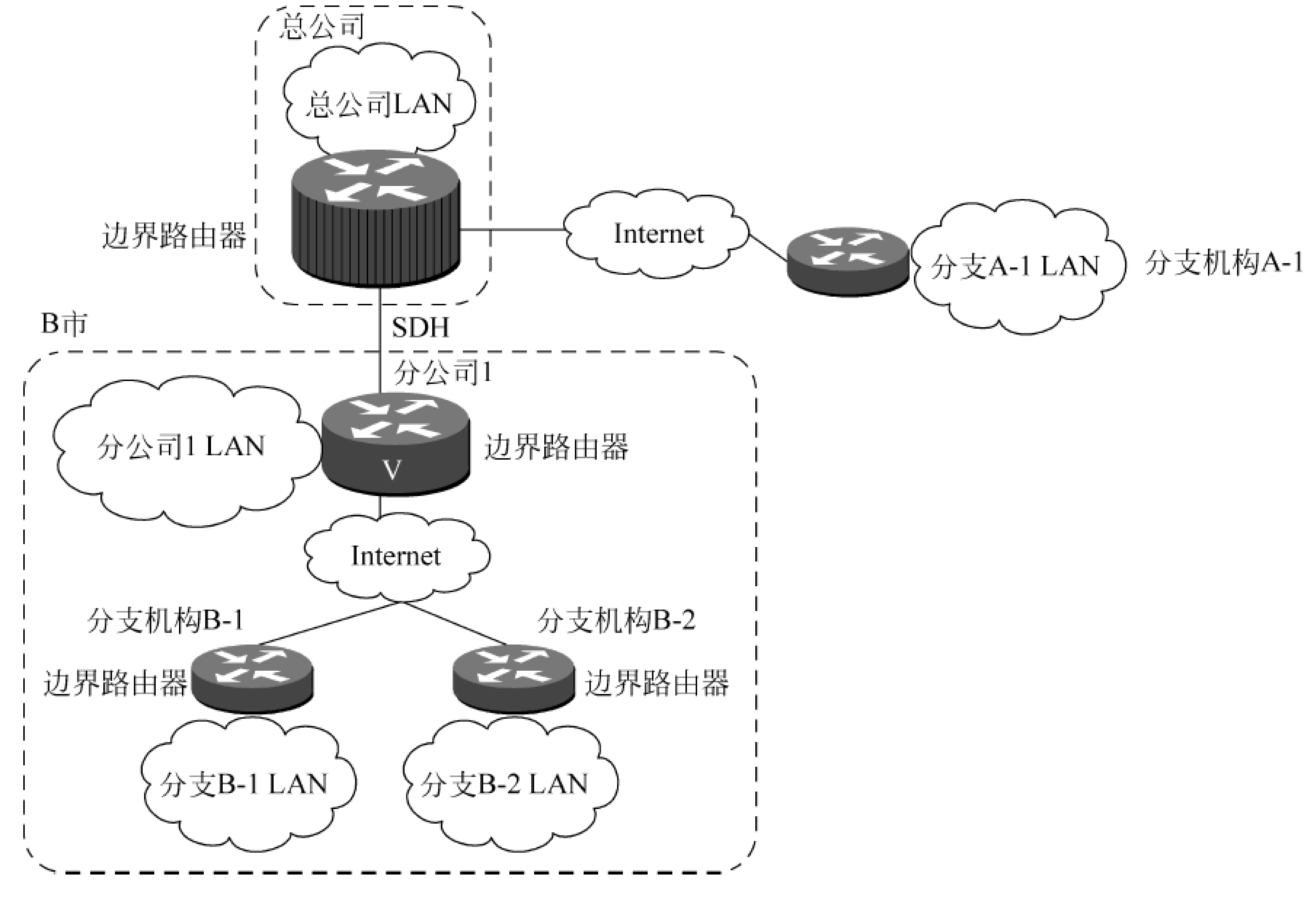


图 5-1　分支机构 B-1 与公司其他单位间的网络连接

- 凡是分支机构 B-1 与模拟分公司 1 间的通信都要受到加密保护；
- 公司职员在 Internet 上对分支机构 B-1 内服务器的远程访问受到加密保护。

更进一步，要求公司所有使用 Internet 线路的网络间进行通信时，均应受到加密保护。

5.2 VPN 简介

5.2.1 VPN 技术及通信安全

VPN(Virtual Private Network，虚拟专用网)技术使用加密、认证等手段，为用户在公共网络上提供了像专用网络一样的通信保障。

在使用 VPN 进行通信的过程中，通信双方经过认证才建立连接；数据报文可以在通信两端被加、解密，只有通信双方可以读取；数据报文被封装在安全协议报文中，附有验证数据，确保在通信过程中对原始数据报文的篡改能够被发现，即数据完整性(Integrity)保证。因此，加密技术、认证技术、数据完整性技术是构成 VPN 的主要内容，也是实施 VPN 时需要配置的部分。

在 VPN 技术中，称使用 VPN 技术建立起来的安全通道为“隧道”(tunnel)，而连接隧道两端，对数据进行安全协议封装、解封装的设备则被称为“对等体”(peer)。

1. 加密技术

(1) 加密技术简介

加密技术是 VPN 技术实现的基础。加密是将明文数据经加密算法处理，转变为难以读取的密文数据的过程；解密则是进行反向操作。

密钥(Key)是一串数字，在加、解密运算过程中，作为参数使用。在通信过程中，可以对数据使用密钥进行加密，使得只有掌握密钥的用户才能解密密文。

根据使用密钥的情况，加密技术分为对称加密、非对称加密两种。

① 对称加密技术。加密、解密时使用同一个单独密钥进行，其工作过程如图 5-2 所示。

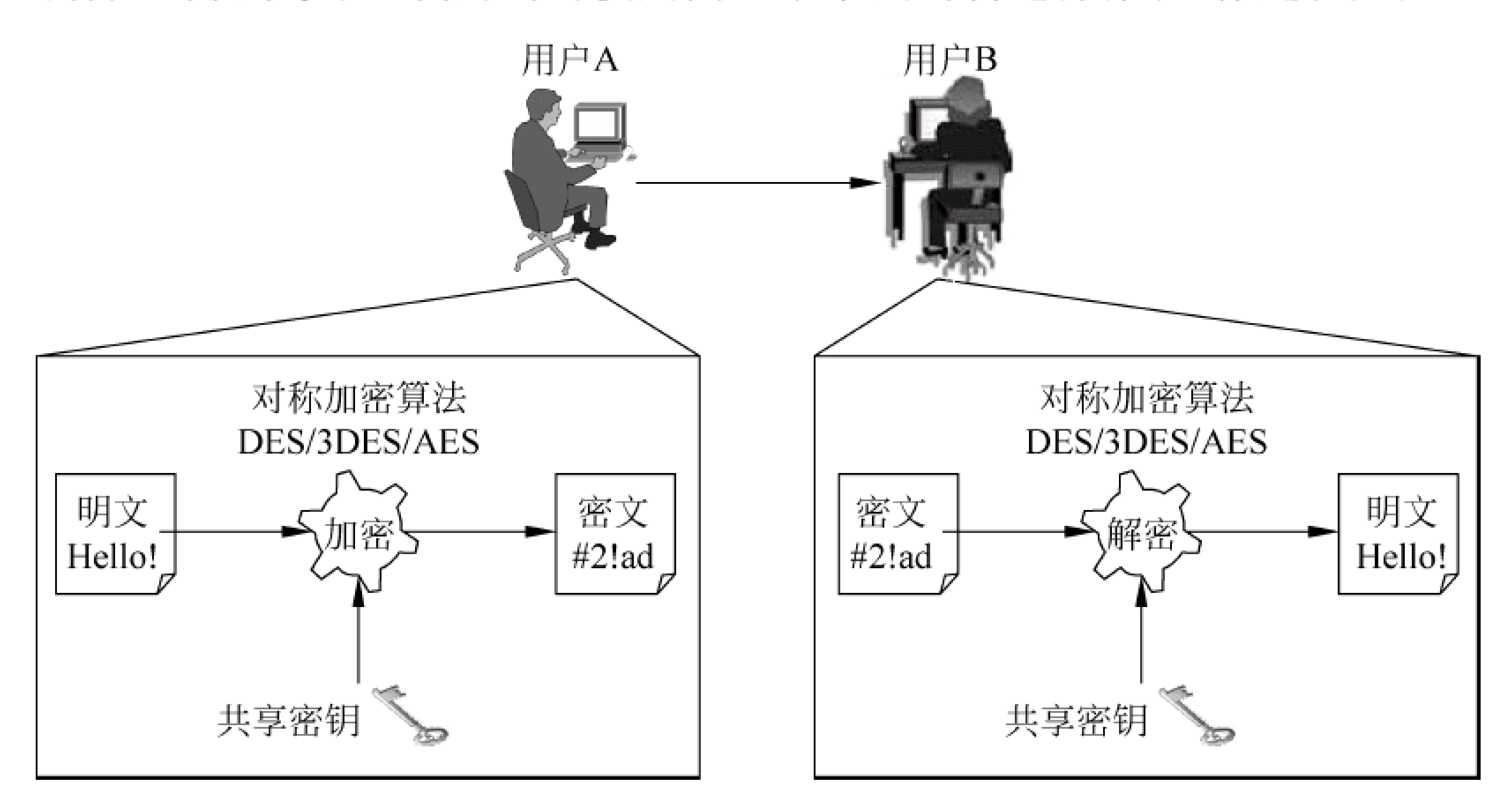


图 5-2 对称加密技术

② 非对称加密技术。使用一对密钥进行加/解密运算，一个密钥用于加密，一个密钥用于解密，其工作过程如图 5-3 所示。用于加密的密钥，被称为私钥；用于解密的密钥，则被称为公钥。注意，使用密钥对中任何一个密钥是不能计算出另一个密钥的。

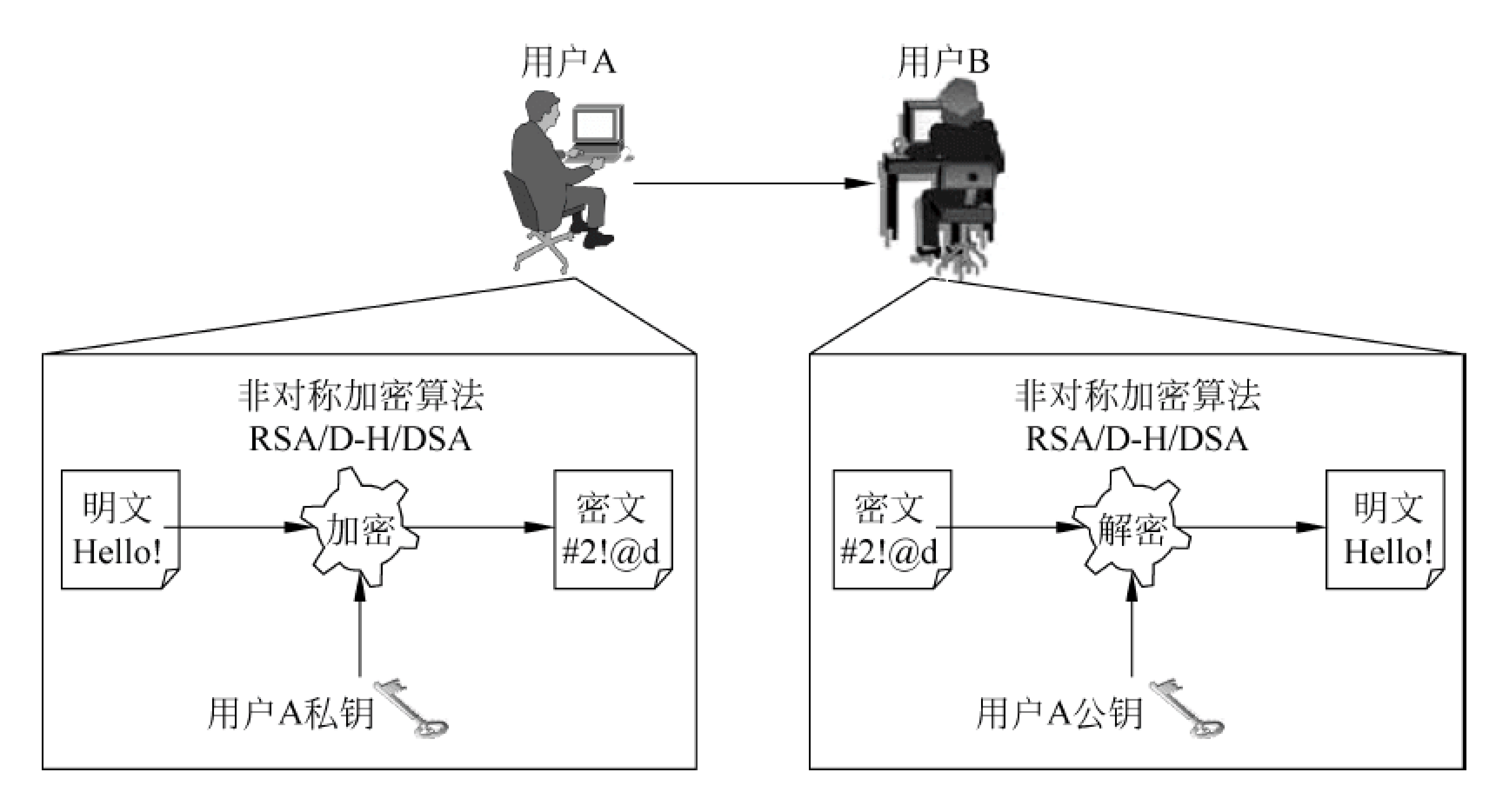


图 5-3 非对称加密技术

加密算法是加密技术的核心。表 5-1 显示了各类常用加密算法的功能及特点。

表 5-1 各类加密算法

类型	算法	功能	抗攻击强度
对称加密	DES	使用 56bit 密钥，加密 64bit 数据块	弱
	3DES	使用 168bit 密钥，加密 64bit 数据块	比 DES 强
	AES	使用 128bit、192bit 或 256bit 密钥，可以加密 128bit、192bit 或 256bit 数据块	比 DES 强
非对称加密	RSA	定义了如何进行密钥交换、数字签名、消息加密的方法	强
	DSA	用于数字签名	
	D-H	定义了如何交换共享密钥的方法	

注意：非对称加密算法一般比对称加密算法运算起来更为复杂、消耗的资源更多，所以在实际应用中，往往将对称加密技术与非对称加密技术结合起来使用。

- 使用对称加密技术加密通信数据，提高加密速度，降低加密所需成本。
- 为防止密钥分配过程中密钥被偷窃，或恶意用户通过统计方法破解共享密钥，每次通信都更换密钥。为使一次性密钥交换更安全、便捷，在密钥分配过程中使用非对称加密技术保护一次性共享密钥。具体方法见下面 D-H 算法。

(2) 密钥交换算法 D-H

在使用共享密钥的通信过程中，需要解决通信用户间安全交换共享密钥的问题。VPN 技术中使用 D-H(Diffe-Hellman，笛夫-哈弗曼)算法解决以上问题。D-H 算法工作原理如图 5-4 所示。

① 用户 A 选择一个素数 p，发送给用户 B。

② 用户 B 使用 p 根据一定规则生成 p 的原根 a，$1<a<p$，并将 a 返回给用户 A。

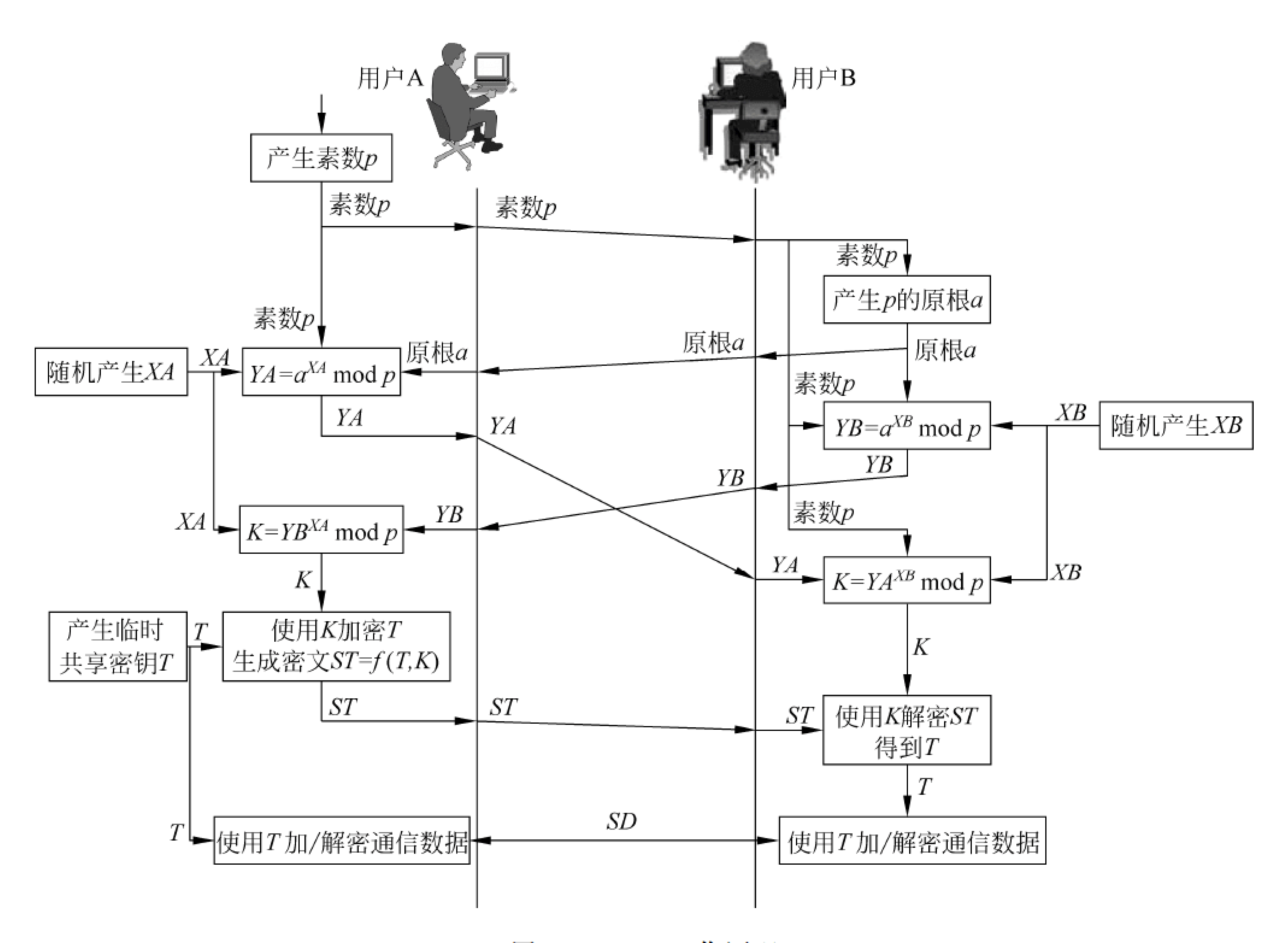


图 5-4　D-H 工作原理

③ 用户 A 随机产生一个不能公开的密钥 XA，并使用 XA、p、a 计算出可以公开的密钥 YA。

④ 用户 B 随机产生一个不能公开的密钥 XB，并使用 XB、p、a 计算出可以公开的密钥 YB。

⑤ 用户 A、用户 B 交换公钥。

⑥ 用户 A 使用 YB、XA 和 p 计算出 K，用户 B 使用 YA、XB 和 p 计算出同样的 K。

⑦ 用户 A 产生一个临时共享密钥 T，并用 K 加密后，发送给用户 B。

⑧ 用户 B 收到用 K 加密的 T 后，使用 K 解密得到 T。

⑨ 用户 A、用户 B 使用 T 加密通信数据，进行通信。

D-H 算法的关键在于，使用 XA、p、a 计算 YA 很容易，而由 YA、p、a 反向计算出 XA 却很难。因此，虽然 D-H 计算过程中公开交换了 p、a、YA、YB 这 4 个数据，但仅截取这些数据很难计算出 XA、XB 和 K；但更为奇妙的是，用户 A、用户 B 能利用此过程生成相同的 K，帮助交换临时密钥 T。由于临时密钥 T 每次通信时才会生成，所以 D-H 算法可以提供很好的机密性。

注意：D-H 算法可以提供交换信息的机密性，但该过程中并没有提供认证机制，所以容易遭受中间人攻击，解决这一问题的办法是在此过程中使用数字证书实现认证的目的。

2. 数据完整性保证

（1）散列

散列也称摘要(Hash)，是一段可以唯一标识通信数据的、固定长度的信息，可以由特定的散列算法，对通信数据进行运算生成。散列具有以下特点。

- 通信数据不同，其散列值不同。
- 不能使用散列反向计算出产生该散列的数据。

由于以上特定，散列被用于在网络通信中鉴别数据完整性，如图 5-5 所示。图中用户 A 发送数据时，附带数据的散列值。用户 B 收到后，重新根据收到的数据用相同的算法计算散列值，如果与收到的散列值相同，则认为数据未被篡改。

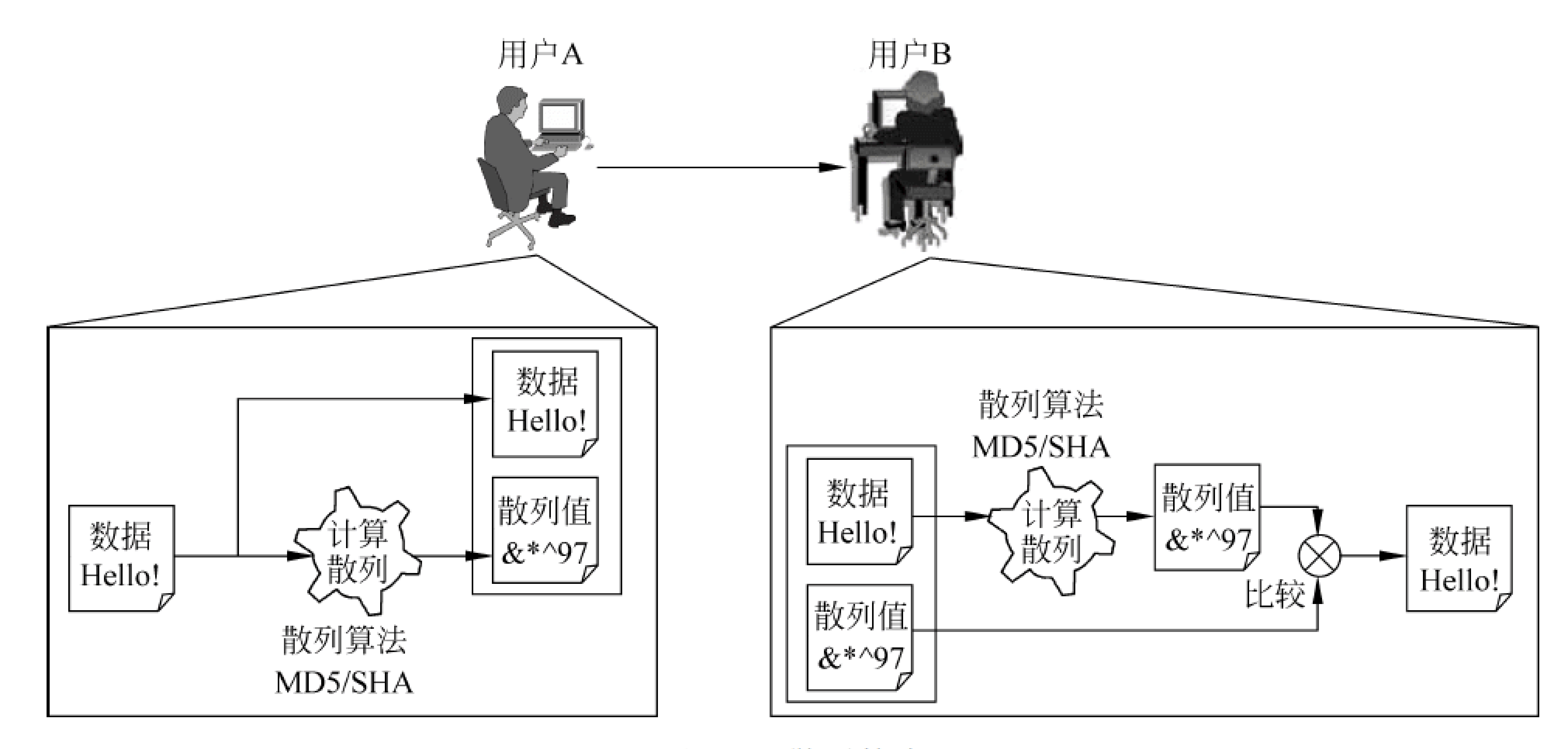


图 5-5 散列技术

一般情况下，抗攻击强度越强的散列算法计算复杂度越高，表 5-2 显示了两种常用的散列算法。MD5 算法虽然抗攻击强度弱，并已被证明 1 小时内就能生成分析攻击和实际冲突，但因为比 SHA 简单，运算速度快，所以仍被很多人使用。

表 5-2 常用散列算法

算法	描 述	抗攻击强度
MD5	被广泛应用于各种应用中，例如 IPSec 等。散列值长度为 65bit	弱
SHA	有 SHA-0、SHA-1、SHA-2 等，其中 SHA-2 又有 SHA-224、SHA-256、SHA-384、SHA-512 多个变体，它们的散列值长度分别为 160bit、160bit、224bit、256bit、384bit 和 512bit。其中 SHA-1 目前广泛用于各种应用中，例如传输层安全协议 TLS、安全套接层协议 SSL、优良保密协议 PGP、安全外壳协议 SSH、IPSec 等	比 MD5 强

（2）散列消息认证码

传统的散列算法生成散列值时不涉及密钥，但散列消息认证码(Hashed Message Authentication Code，HMAC)生成散列值时，却将一个共享密钥附加在消息上，一同计算散列值，如图 5-6 所示。HMAC-MD5 和 HMAC-SHA-1 是两种常用的 HMAC 算法，分别生成 128bit 和 160bit 长度的散列值。如前所述，HMAC-MD5 在抗攻击强度方面不如

HMAC-SHA-1。

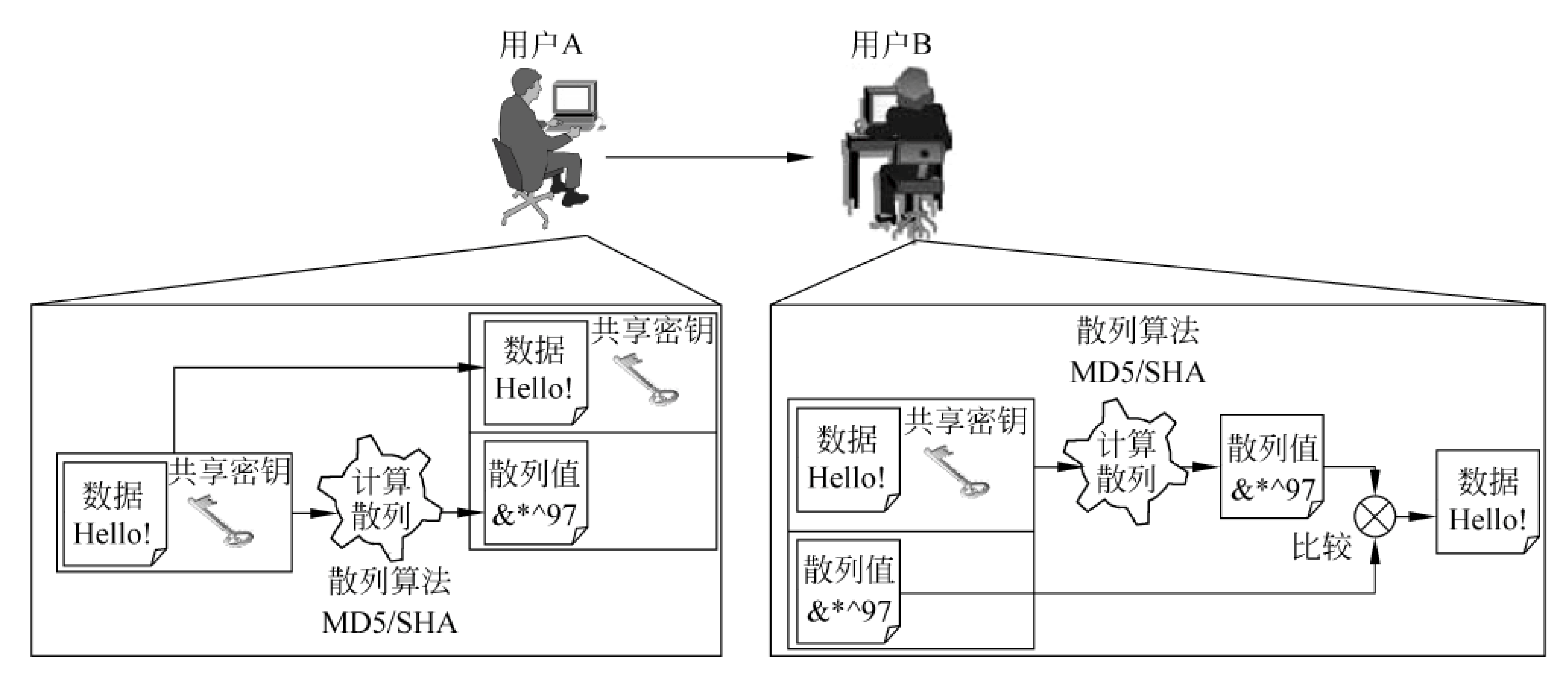


图 5-6　HMAC 过程

在 VPN 技术中，散列消息认证码被用于验证通信数据是否在通信过程中受到了破坏。

（3）数字签名及数字证书

在非对称加密技术中，私钥由用户自己保存，而公钥可以公开给通信接收者解密数据使用。由于只有用户自己持有私钥，并且只有使用该用户的公钥才能解开用其私钥加密的数据，所以私钥加密通信数据生成的密文被称为“数字签名”，可以被通信数据的接收者用来判断发送数据用户的身份。同时，接收者也可以通过比较接收的数字签名和由接收数据产生的数字签名是否一致，来判断通信数据是否在网络传输过程中被破坏。使用数字签名保证通信数据完整性的过程如图 5-7 所示。图中，用户 A 将带有通信数据、通信数据数字签名以及用户 A 数字证书的报文发送给用户 B。用户 B 从用户 A 数字证书中提取用户 A 的公钥，然后用该密钥加密收到的数据，并将由此得到的数字签名与收到的通信数据进行比较，如果相同则认为数据未被破坏。

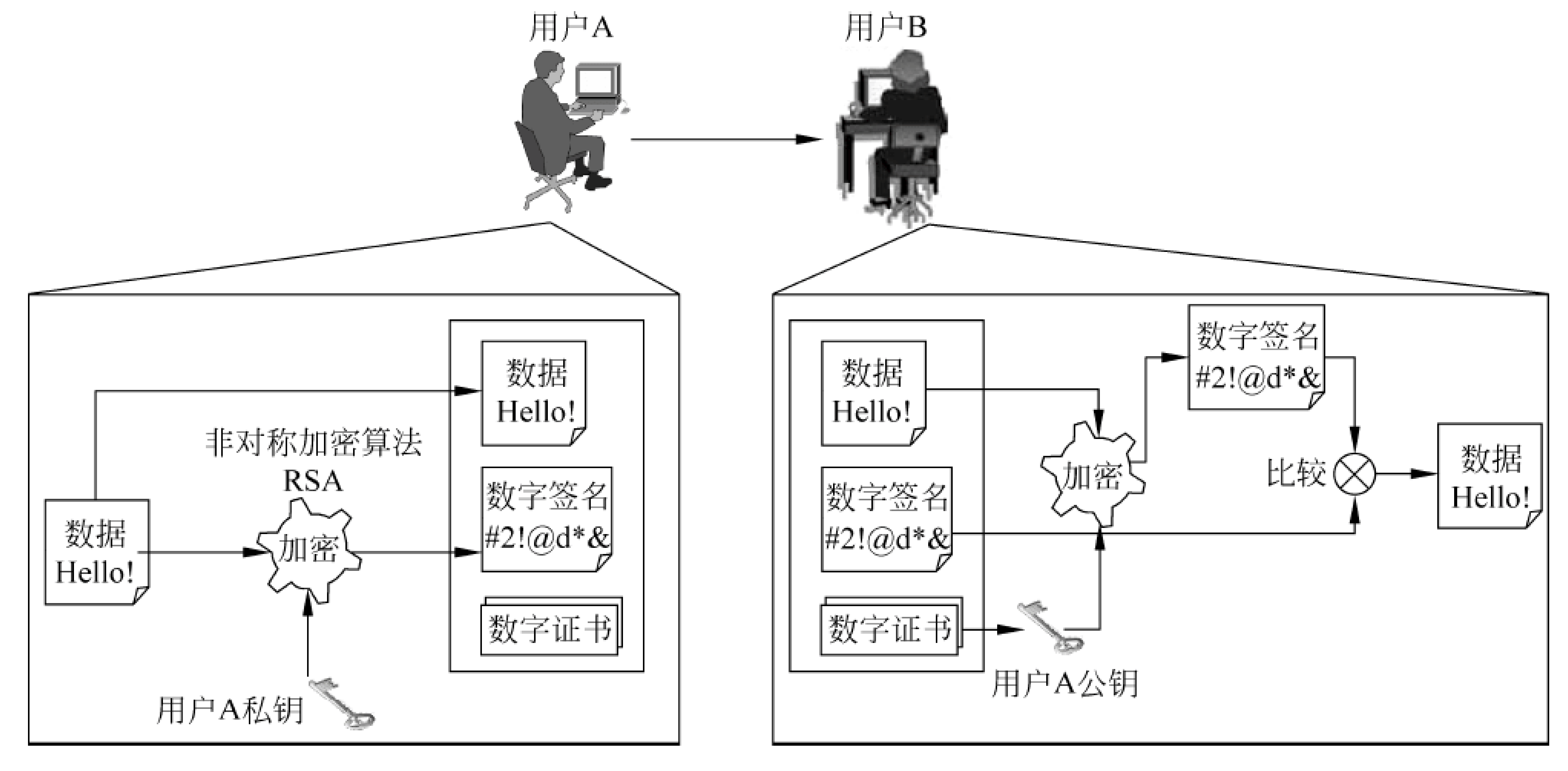


图 5-7　使用数字签名保护数据完整性

在网络通信中，为将用户密钥与用户真实社会身份结合起来，引入了数字证书技术。

数字证书技术的核心是基于非对称加密技术的“信任传递”机制，也被称为 PKI(公开密钥基础设施)。“信任传递”机制的原理是：通信双方都信赖 CA(Certificate Authority，认证中心，可信第三方)，则由 CA 进行数字签名的信息(用户身份信息＋用户公钥)是可信的。数字证书就是一串包含用户身份信息、用户公钥和 CA 数字签名的数字，其主要内容如下。

- 证书序列号。
- 证书有效期。
- 证书颁发机构名称。
- 证书申请者的名称、组织机构信息或者 IP 地址等信息。
- 证书申请者的公钥。
- 证书颁发机构对以上信息所做的数字签名。

获得数字证书和验证数字证书的过程如图 5-8 所示。

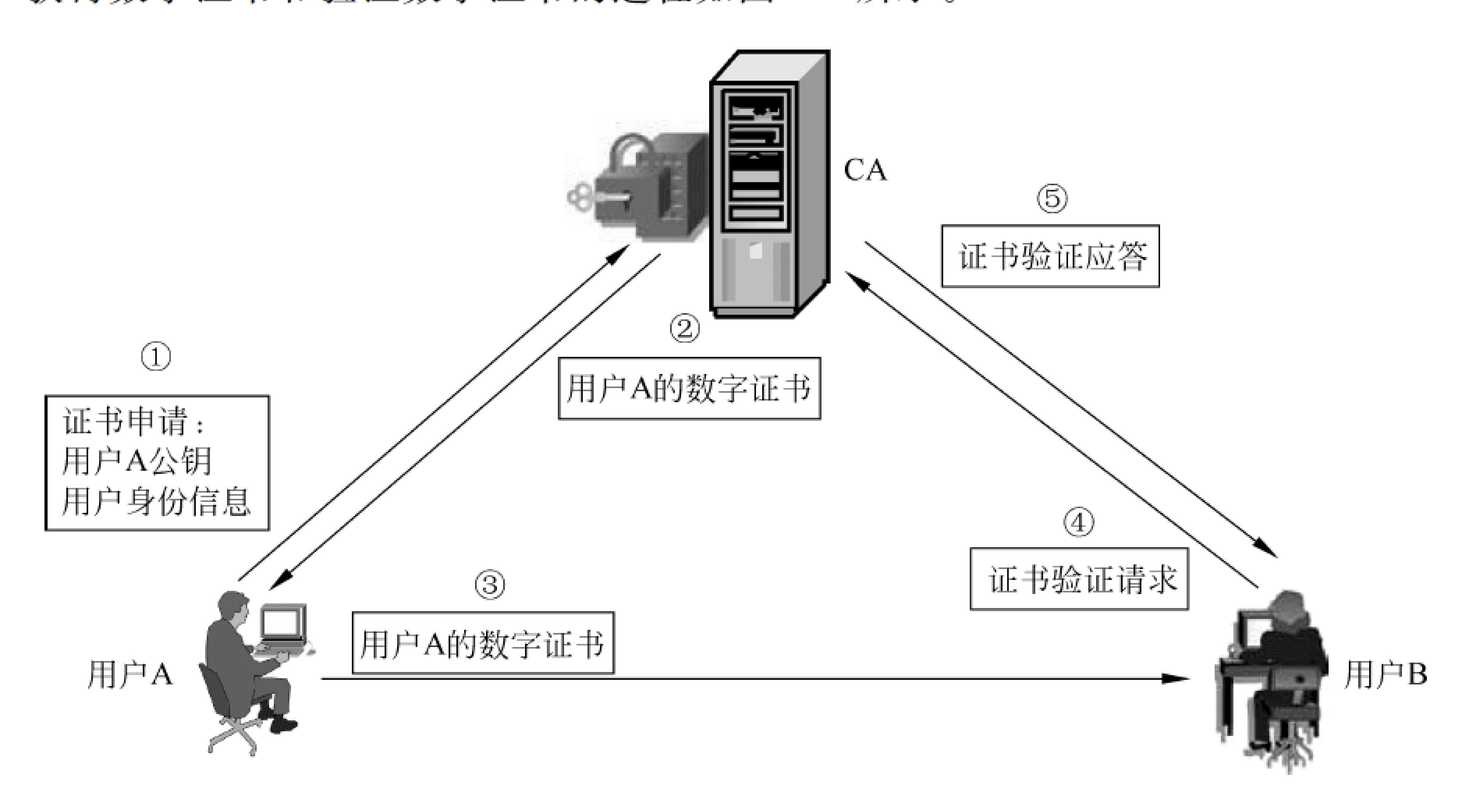


图 5-8 验证数字证书

① 用户 A 生成自己的非对称密钥对(Key-private，Key-public)；用户 A 将非对称密钥对中的公钥 Key-public 和自己的身份信息提供给第三方认证机构 CA；CA 核对用户身份信息是否属实；CA 用自己的私钥对用户身份信息和用户公钥进行加密，生成数字签名，证明这些信息已经被自己认可。

② CA 制作用户 A 的数字证书，并将证书制作信息保存在其数据库中，然后将制作好的数字证书发送给用户 A。

③ 用户 A 将自己的数字证书发送给用户 B(用户 B 也可以通过其他方式获取用户 A 的数字证书)。

④ 用户 B 收到数字证书，但希望能证明该数字证书是否真实有效，因此向颁发证书的 CA 发出验证请求。

⑤ CA 根据证书序列号在证书数据库中查找有关记录，检查用户 A 数字证书中的数

字签名是否由自己签发、用户 A 的数字证书是否已经过期等，并向用户 B 返回检查结果。

3. 认证技术

认证是对通信用户身份进行确定的过程。VPN 对等体在建立安全隧道前先要彼此进行认证，其所使用的认证方式主要有以下 3 种。

(1) 预共享密钥。

(2) RSA 加密随机数。

(3) 数字签名。

4. VPN 种类

根据不同因素，可以对实现 VPN 的技术进行多种分类。

根据是否对通信进行加密，分为加密 VPN 和非加密 VPN。

- 典型的加密 VPN 有 IPSec、SSL 加密。
- 典型的非加密 VPN 有 GRE、MPLS VPN。

限于篇幅，本书仅选择介绍工程中应用最多的 IPSec VPN。

根据 VPN 拓扑形式不同，VPN 又分为站到站的 VPN 和远程访问 VPN 两种。

- 站到站 VPN 也称为网络到网络 VPN，VPN 安全隧道两端连接的设备功能对等，建立安全隧道时需要远端对等体的 IP 地址。站到站 VPN 常在两个网络的边界路由器上配置。
- 当用户使用 Internet 线路访问公司网络时，一般 IP 地址不固定，无法使用站到站方式，根据站点 IP 地址建立安全关联；同时对用户的配置要求过多。远程访问 VPN 可以解决这一问题。根据发起 VPN 连接者不同，远程访问 VPN 又分为客户端发起、NAS 发起两种。客户端发起 VPN，是指用户使用一个 VPN 客户端或 Web 浏览器在公网上建立到达公司网络 VPN 安全隧道；NAS 发起 VPN，是指用户首先拨入一个 ISP 网络接入服务器(NAS)，然后由 NAS 建立一条到达公司网络安全隧道，即 VPN 连接是由 NAS 代为发起的。这种隧道可以支持由远程用户发起的多个会话。

5.2.2　IPSec VPN

IPSec (IP Security，IP 安全)是一个安全框架，定义了一套保护 OSI 模型第三层 IP 流量的协议。主要包括以下内容。

- 建立安全隧道前协商安全隧道各项参数的协议，如 ISAKMP 和 IKE。
- 安全隧道本身使用的数据封装协议，如 ESP、AH。

1. IPSec 模式

在 IPSec 中，定义了以下两种传输数据的模式。

- 隧道模式(tunnel)：保护网络到网络间的 IP 流量，如图 5-9 所示。
- 传输模式(transport)：保护主机间或端到端的流量，如图 5-10 所示。

隧道模式在两个网络间建立 IPSec 隧道，所有经过 IPSec 对等体(图 5-9 中两个网络的边界路由器被配置为 IPSec 对等体)进入隧道的 IP 报文，先被整个加密，然后被封装上一个新 IP 报头，最后在新 IP 报头后插入添加 IPSec 头，如图 5-11 所示。

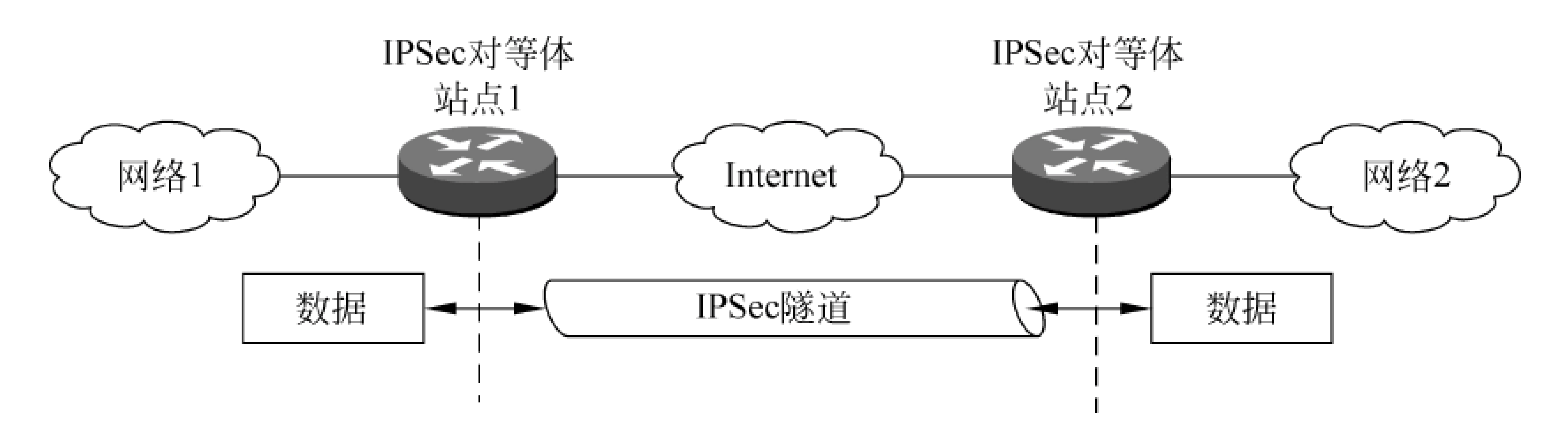


图 5-9　IPSec 隧道模式

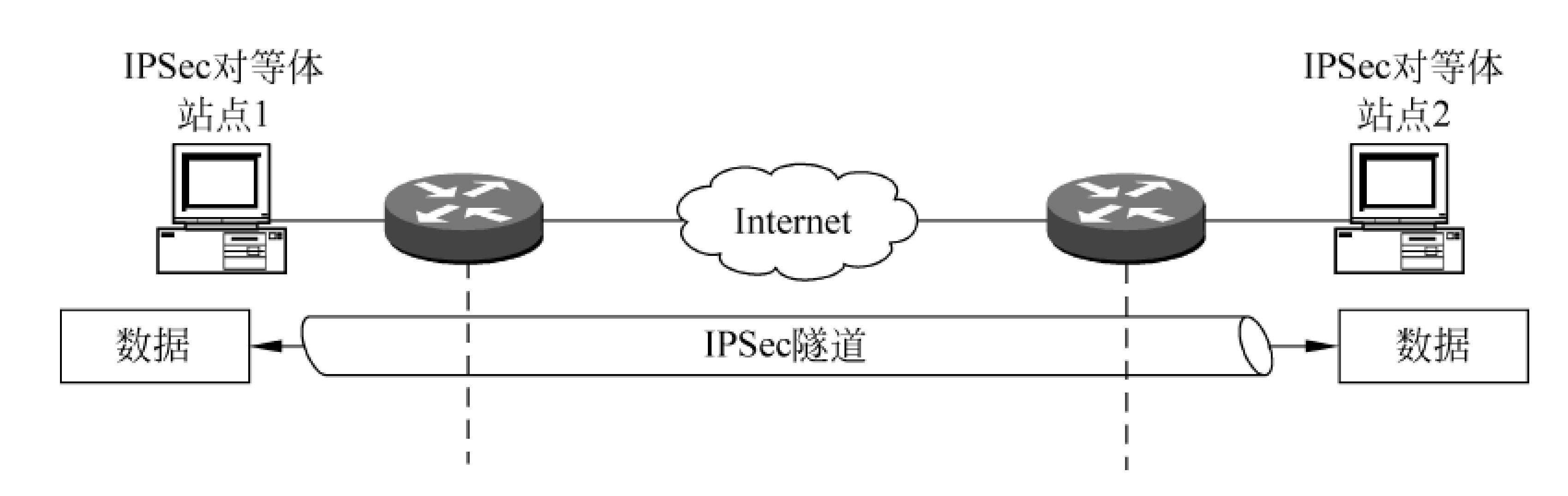


图 5-10　IPSec 传输模式

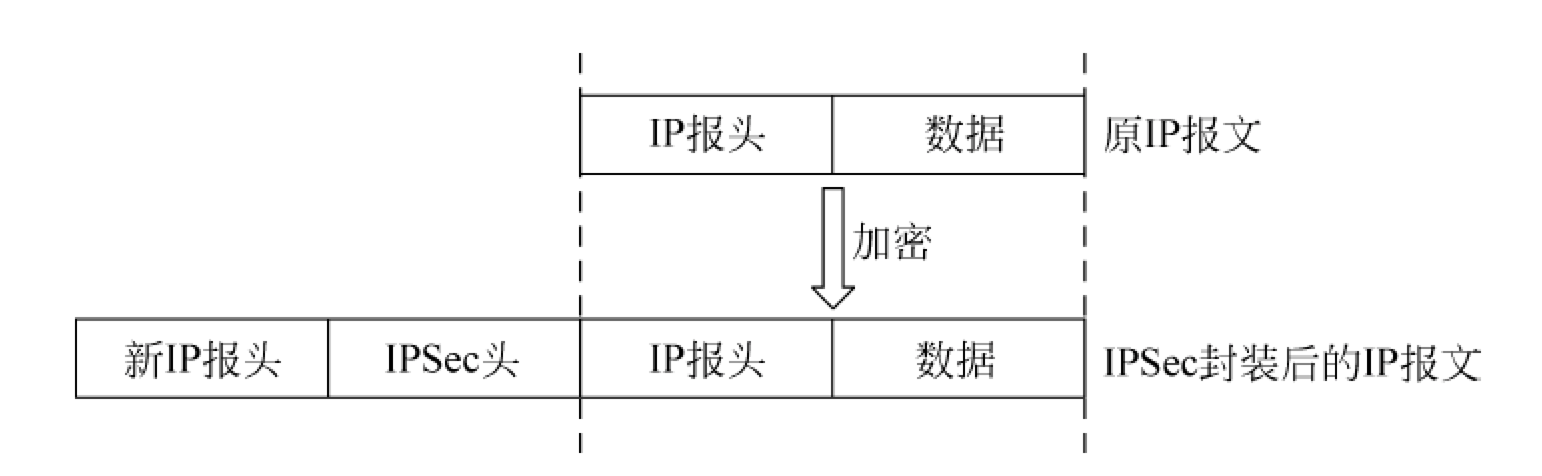


图 5-11　隧道模式报文结构

传输模式在两个主机间建立 IPSec 隧道，所有经过对等体(图 5-10 中两台主机被配置为 IPSec 对等体)进入隧道的 IP 报文，IP 报头不改变，IP 报头后被插入一个 IPSec 报头，IP 报文上层协议数据被单独加密，如图 5-12 所示。

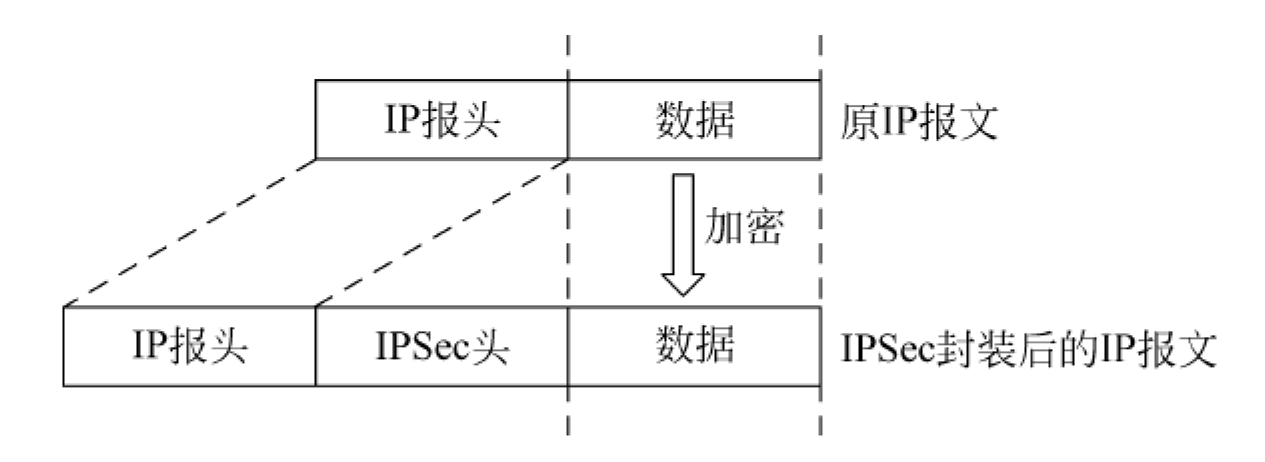


图 5-12　传输模式报文结构

2. IPSec 封装协议

IPSec 有两种封装协议：ESP(Encapsulating Security Payload，封装安全载荷)协议和 AH(Authentication Header，认证头)协议。

（1）AH 协议

AH 协议的 IP 协议号为 51，它提供报文验证、完整性保证及重放探测/保护等安全服务，但不提供机密性和加密。图 5-13 所示为 AH 报头结构。

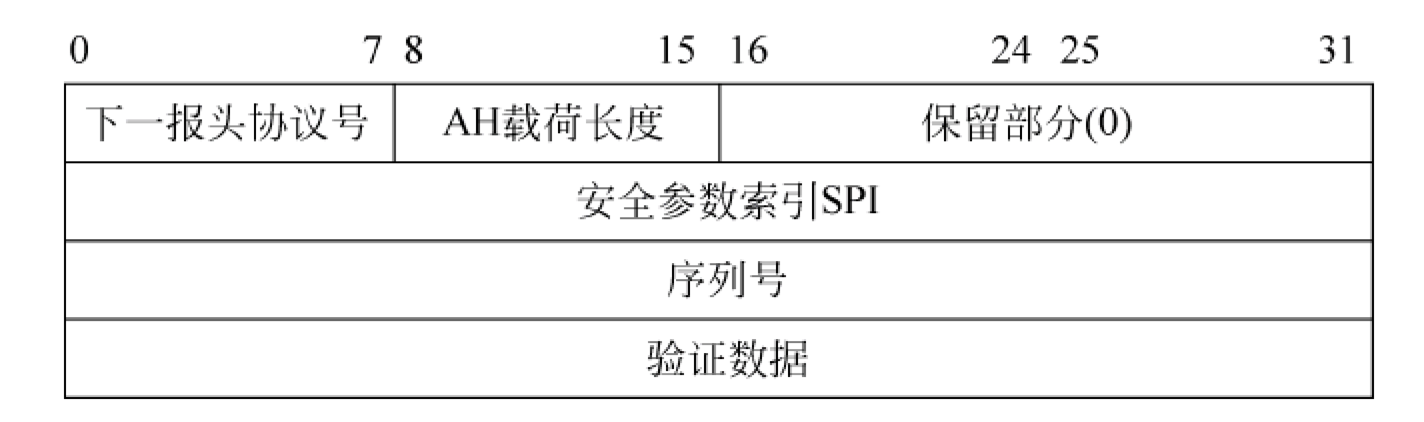


图 5-13　AH 报头结构

① 如图 5-14(a)所示，AH 报头作为 IPSec 报头，插入在 IP 报头与 IP 数据字段间，AH 报头中的"下一报头协议号"用于指定 IP 数据字段中上一层协议的协议号。例如，如果 IP 数据字段中是 TCP 协议报文，则此处为 6。

② "AH 载荷长度"定义整个 AH 报头的长度，最小为 2，以 32bit 为单位。

③ "保留部分"为 16bit，默认为全 0。

④ "安全参数索引 SPI"为该报文使用的 SA（Security Association，安全关联）标识。

⑤ "序列号"可以防止重放攻击。

⑥ "验证数据"（Integrity Check Value，ICV，完整性验证值）部分存放 AH 对以下几部分信息的验证值。

- IP 报头。
- AH 报头，其中验证数据部分在计算时置 0。
- 上层协议数据。

在不同传输模式下，AH 验证范围如图 5-14 所示。

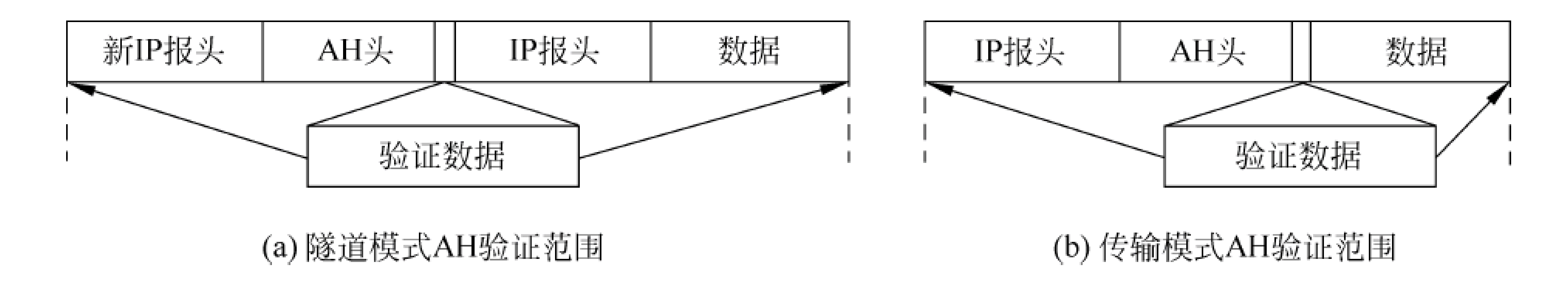


图 5-14　AH 验证范围示意图

注意：由于 AH 对 IP 报文整体进行验证，包括 IP 报头中的 IP 地址，所以在 AH 协议封装的 VPN 隧道上使用地址转换时，会出现验证错误。

（2）ESP 协议

ESP 协议的 IP 协议号为 50。ESP 协议可以提供数据机密性、完整性和真实性、反重放保证等安全服务。图 5-15 显示了 ESP 协议封装结构。

使用 ESP 协议重新封装 IP 报文时，结构比较复杂一些。图 5-16 和图 5-17 显示了不同模式下 ESP 重新封装 IP 报文的结构以及 ESP 加密、验证处理的范围。

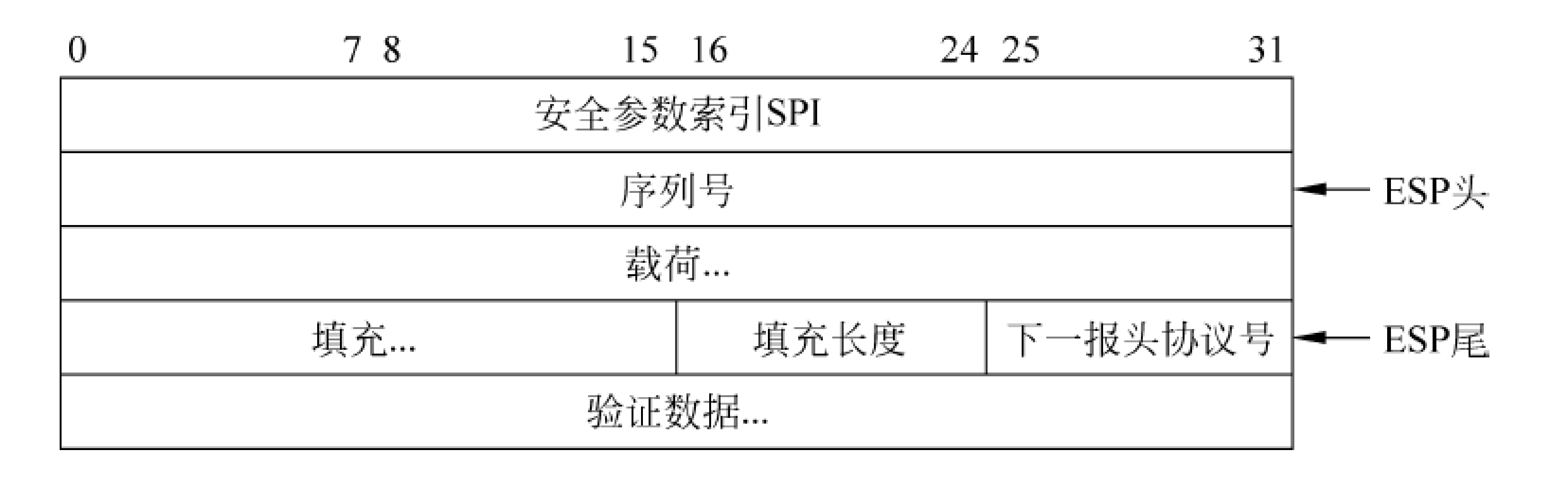


图 5-15　ESP 协议报文封装结构

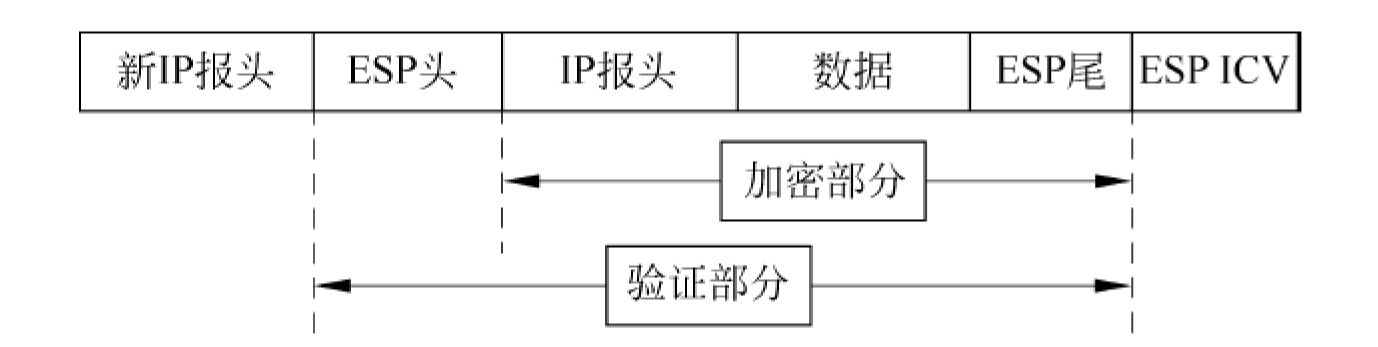


图 5-16　隧道模式 ESP 封装及机密验证范围

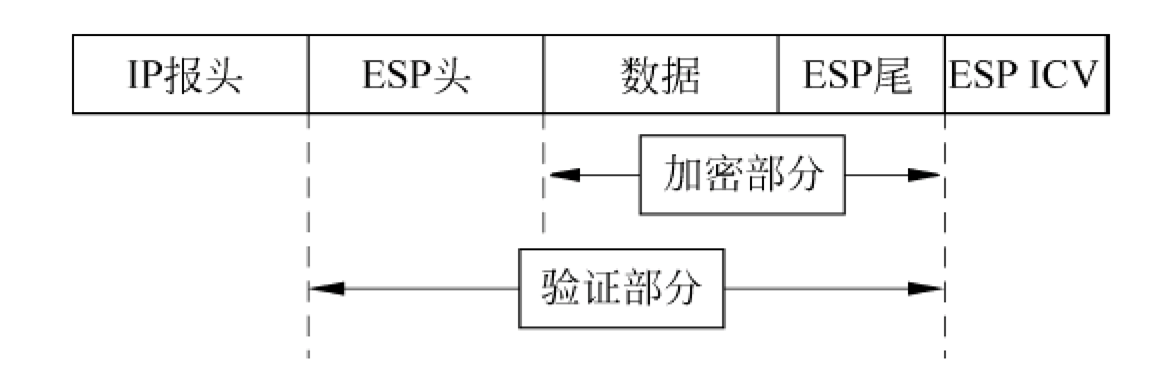


图 5-17　传输模式 ESP 封装及机密验证范围

（3）AH 与 ESP 协议的选用

由于 AH 不提供对通信数据进行加密的服务，所以一般不会单独使用 AH，而是与 ESP 一同配合使用，如表 5-3 所示。在配置 IPSec VPN 时，可以参考该表选择恰当的安全参数选项。

表 5-3　IPSec 封装协议选项

	选择 1	选择 2
封装协议	ESP	AH＋ESP
加密算法	DES	3DES
散列算法	MD5	SHA
密钥交换算法（D-H 算法）	DH1	DH2

3．IPSec 密钥决策和密钥交换机制

IPSec VPN 中可以对通信数据进行加密，因此在 IPSec VPN 隧道建立前，需要解决对等体识别、密钥协商和密钥交换问题。IPSec 使用 ISAKMP 和 IKE 两个协议来解决此问题。

(1) ISAKMP

ISAKMP(Internet Security Association and Key Management Protocol,Internet 安全关联和密钥管理协议)描述了密钥管理的框架,并定义了建立、协商、修正和删除安全关联 SA 的程序和分组格式。SA 是 VPN 中两个对等体间使用的安全策略,包含对等体间传输安全协议报文所需的安全参数。

注意:ISAKMP 提供了对等体识别和建立 SA 功能,但不提供密钥交换机制。

(2) IKE

IKE(Internet Key Exchange,Internet 密钥交换)协议是一个组合了 ISAKMP、Oakley 密钥转换和 SKEME 等协议的混合型协议,定义了对等体识别和密钥交换机制。IKE 协议使用 UDP 500 端口通信。

IKE 定义了一个两阶段工作模型。第 1 阶段先在对等体间建立一个用来交换管理信息的安全通道 ISAKMP SA;第 2 阶段在第 1 阶段建立的安全通道上交换信息,并最终在对等体间建立真正用于传输业务数据的安全通道 IPSec SA。

第 1 阶段 IKE 协商的主要内容如下。

- 第 1 阶段使用的加密、散列算法。
- 使用 D-H 算法生成的会话密钥。
- 验证方法。
- 第 2 阶段使用的密钥。

IKE 第 1 阶段通信可以选择使用主模式或者野蛮模式进行。野蛮模式比主模式快,但安全性不如主模式。图 5-18 显示了使用主模式的 IKE 第 1 阶段协商过程,图 5-19 显示了使用野蛮模式的 IKE 第 1 阶段协商过程。

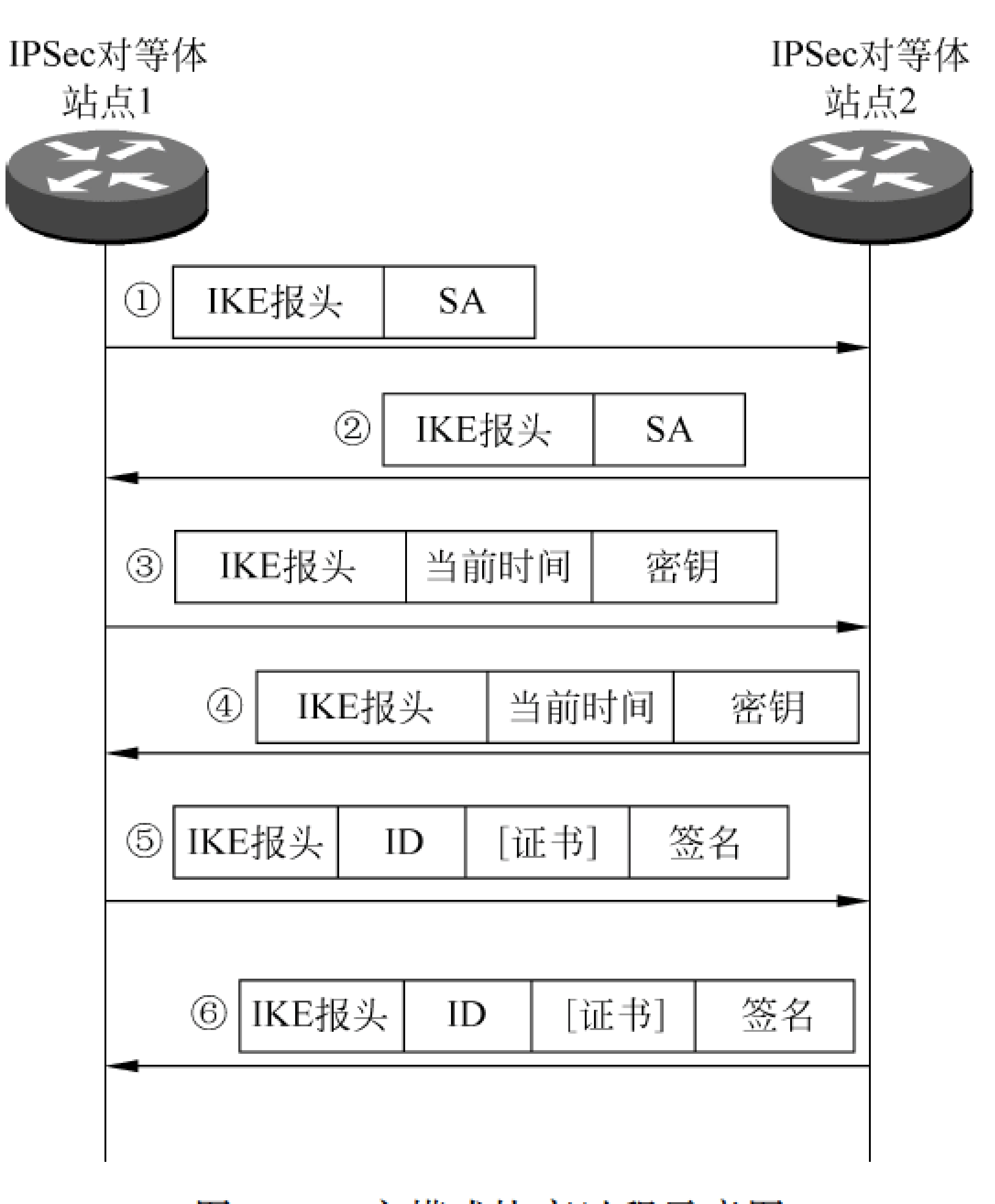


图 5-18　主模式协商过程示意图



图 5-19 野蛮模式协商过程示意图

① 站点 1 从本地配置的 ISAKMP/IKE 策略中选择一个策略，发送给站点 2。其中包括加密与验证使用的算法，如 3DES、MD5、RSA 等。ISAKMP/IKE 策略中定义了创建第 1 阶段 ISAKMP SA 的有关参数。

② 站点 2 从本地配置的 IKE 策略中查找匹配的策略，并返回是接受还是拒绝站点 1 发出策略的响应。如果站点 2 接受了站点 1 策略，则进入下一步。

以上两步主要用于协商建立安全通道所用的算法等。

③～④ 站点 1、站点 2 使用 D-H 算法交换密钥。

⑤～⑥ 站点 1、站点 2 发送数字证书、签名等进行对等体身份认证，同时将其他 SA 参数发送给对方。

①～② 站点 1、站点 2 间进行密钥交换，并协商建立 ISAKMP SA 的参数。

③ 站点 1 向站点 2 对等体进行身份认证。

IKE 第 2 阶段使用快速模式在对等体间进行协商，建立数据传输的 IPSec SA，第 2 阶段协商的内容如下。

- 通信隧道封装协议(ESP 或 AH)。
- ESP、AH 中使用的加密、散列算法(DES、3DES、AES、SHA 等)。
- 要保护的网络或 IP 流量。
- 协商可选的密钥参数。

IKE 第 2 阶段协商过程如图 5-20 所示。



图 5-20 IKE 快速模式协商过程示意图

4. IPSec VPN 运行步骤

IPSec VPN 的运行分为以下 5 个工作步骤。

(1) 当被指定受 VPN 保护的流量经过网络设备时,网络设备被触发建立 VPN 安全隧道。

注意: 由于加密、解密运算非常耗费网络通信设备的资源;加密、解密处理也增加了通信处理环节,加大了数据传输时延,因此只加密、解密需要保护的数据,是规划和设计 VPN 实施方案时必须考虑的内容。

(2) 网络设备根据 VPN 配置,作为对等体与另一远端对等体进行 IKE 第 1 阶段协商,建立一条 ISAKMP SA 安全连接通道,用于保护第 2 阶段 IKE 协商。

(3) 网络设备作为对等体在已建立的 ISAKMP SA 安全连接通道上协商建立 IPSec SA。

(4) 网络设备作为对等体在已建立的 IPSec SA 上传输数据,按照协商的定义,使用 ESP、AH 协议处理通信数据。

(5) 在 IPSec 隧道终结时,删除或终结 IPSec SA,释放资源。

5.3 IPSec VPN 配置

根据前述对 IPSec 主要构成技术及运行步骤介绍不难发现,要构建 IPSec VPN,一定需要配置以下几项内容。

- 在哪些网络、主机间建立 IPSec VPN 安全隧道。
- 建立 ISAKMP SA 所需的各项参数。
- 建立 IPSec SA 所需的各项参数。
- 将 IPSec SA 与所要保护的网络、主机绑定在一起。
- 指定网络设备哪个接口来处理 IPSec VPN。

5.3.1 站到站 VPN 配置

配置站到站 VPN,需要在两端对等体上同时配置相匹配的 ISAKMP SA 和 IPSec SA 的参数,当使用预共享密钥进行认证时,还需要在两个对等体上配置相同的预共享密钥。

在 Cisco IOS 路由器上配置预共享密钥站到站 VPN 的步骤如表 5-4 所示。

表 5-4　预共享密钥站到站 VPN 配置步骤

序　号	操　作	相关命令	必要
步骤 1	检查网络访问控制,确保 IPSec 报文被允许通过	**show ip access-list**	可选
步骤 2	定义建立 ISAKMP SA 所需的各项参数	**crypto isakmp policy** 及其子命令 **group**、**authentication**、**encryption**、**hash**、**lifetime**	是
步骤 3	定义对等体间预共享密钥	**crypto isakmp key**	是
步骤 4	定义建立 IPSec SA 所需的各项参数	**crypto ipsec transform-set**	是

续表

序　号	操　　作	相关命令	必要
步骤 5	定义受到 VPN 保护的流量	**ip access-list** 或 **access-list**	是
步骤 6	定义加密图，将安全策略与要保护的对象绑定在一起；定义 IPSec SA 所需的其他参数	**crypto map**	是
步骤 7	将加密图应用到正确接口上	接口模式下的 **crypto map**	是
步骤 8	检查 VPN 配置	**show crypto isakmp policy** **show crypto ipsec transform-set** **show crypto ipsec sa** **show crypto map** **debug crypto ipsec** **debug crypto isakmp**	可选

1. 定义建立 ISAKMP SA 所需的各项参数

Cisco 网络设备将建立 ISAKMP SA 所需各项参数保存在一个称为"ISAKMP 策略"的数据结构中。因此，定义这些参数的操作就是定义一个 ISAKMP 策略。

在 Cisco IOS 路由器上，定义一个 ISAKMP 策略的操作是在全局配置模式下输入：

crypto isakmp policy ISAKMP/IKE 策略优先级

然后在其子模式下输入子命令：

group 1 | 2 | 5
authentication 认证方式
encryption 加密算法
hash 散列算法
lifetime ISAKMP SA 生存时间

"ISAKMP/IKE 策略优先级"参数：在 Cisco 网络设备上可以配置多个 ISAKMP/IKE 策略，供协商时选用。网络设备会根据 ISAKMP/IKE 策略优先级顺序依次将其发送到远端对等体进行协商。由于只有两端对等体 ISAKMP/IKE 策略一致，才能建立 ISAKMP SA，从而进入 IKE 第 2 阶段。所以在配置站到站 VPN 时，必须保证至少能在本地找到一个 ISAKMP/IKE 策略。如果对等体上自定义的 ISAKMP 策略都协商失败，则系统还会尝试使用默认的 ISAKMP 策略进行协商。

group 子命令用于定义进行安全参数协商时，使用哪种 D-H 算法交换通信密钥，可以选择 1、2 或者 5。该值取自于 IPSec 框架中关于 D-H 算法的有关定义。D-H 算法以一个素数 p 作为计算基础，p 越大，破解其交换的密钥的难度越大。素数 p 长度可以为 768bit、1024bit、1536bit 等，在 IPSec 框架中被分别定义为 D-H 组 1、D-H 组 2、D-H 组 5。可见选用的 D-H 组号越大，保护密钥能力越强，但相应计算的速度会越慢。

authentication 子命令用于定义使用哪种方式进行对等体身份认证。如前所述，有 3 个选项：预共享密钥方式 pre-share、RSA 加密随机数方式 rsa-encr 和 RSA 数字签名方式 rsa-sig。使用预共享密钥方式时，选择 pre-share。

encryption 子命令用于定义使用哪种加密算法加密 IKE 第 1 阶段协商过程中对等体间的通信，可以选择 des、3des 或者 aes。

hash 子命令用于定义使用哪种散列算法对 IKE 第 1 阶段对等体间的通信进行完整性保证。可以选择 md5 或者 sha。

lifetime 子命令用于定义 ISAKMP SA 的生存时间。单位为秒，取值范围为 60～86400。

例如，创建优先级为 100 的 ISAKMP/IKE 策略，使用 DES 加密算法、MD5 散列算法、预共享密钥方式进行对等体间认证，使用 768bit D-H 算法和默认的 SA 生存时间，则可以如下操作。

```
R0(config)#crypto isakmp policy 100
R0(config-isakmp)#encryption des
R0(config-isakmp)#hash md5
R0(config-isakmp)#authentication pre-share
R0(config-isakmp)#group 1
R0(config-isakmp)#lifetime 86400
```

2. 定义预共享密钥

在 Cisco IOS 路由器上，定义预共享密钥的操作是在全局配置模式下输入：

crypto isakmp key 预共享密钥 [**address** 远端对等体 IP 地址 远端对等体子网掩码 | **hostname** 远端对等体主机名]

参数“远端对等体 IP 地址”或参数“远端对等体主机名”用于定义该密钥在与对等体间建立安全隧道时使用。

例如，在模拟分公司边界路由器上配置到分支机构 B-1 站到站 VPN 时，如果与分支机构 B-1 对等体间认证使用的密钥是“@-B-!”，分支机构 B-1 端接口 IP 为 200.100.15.205，则配置预共享密钥的操作是：

```
R0(config)#crypto isakmp key @-B-! address 200.100.15.205
```

3. 定义建立 IPSec SA 所需各项参数

在 Cisco IOS 路由器上，定义 IKE 第 2 阶段各项安全参数的操作是在全局配置模式下输入：

crypto ipsec transform-set 变换集名 { ESP 加密算法及参数 | ESP 验证算法 | AH 验证算法 } [...]

IKE 第 2 阶段需要定义建立 IPSec SA 的有关参数，如封装协议等。由于是将原 IP 报文变换为 IPSec 报文，所以 IPSec 中将此部分参数的集合称为“变换集”。

参数“变换集名”是一串字符串，必须以字母开头，用于定义该变换集在网络设备上的唯一标识。

在定义 IPSec SA 时，可根据实际需要选择是否进行加密和验证。如前所述，VPN 隧道可以使用 AH 封装，也可以使用 AH＋ESP 封装，所以可以在一个加密集中同时定义 AH 验证算法、ESP 加密算法和 ESP 验证算法。各算法参数可用值如表 5-5 所示。

表 5-5 网络设备支持的 AH、ESP 算法

算法	可用值	含义
AH 验证算法	ah-md5-hmac	使用 AH 协议封装 IP 报文,并使用基于 MD5 的 HMAC 作为验证算法
	ah-sha-hmac	使用 AH 协议封装 IP 报文,并使用基于 SHA 的 HMAC 作为验证算法
ESP 加密算法	esp-3des	使用 ESP 协议封装 IP 报文,并使用 3DES 作为加密算法
	esp-aes	使用 ESP 协议封装 IP 报文,并使用 AES 作为加密算法。选择此加密算法时,可以选择使用 128bit、192bit 还是 256bit 长度的密钥
	esp-des	使用 ESP 协议封装 IP 报文,并使用 DES 作为加密算法
ESP 验证算法	esp-md5-hmac	使用 ESP 协议封装 IP 报文,并使用基于 MD5 的 HMAC 作为验证算法
	esp-sha-hmac	使用 ESP 协议封装 IP 报文,并使用基于 SHA 的 HMAC 作为验证算法

例如,如果要使用 AH+ESP 封装 IP 报文,且 AH、ESP 均使用 SHA 作为验证算法,ESP 使用 128bit AES 加密算法,则可以如下操作定义一个名为 12b 的变换集。

R0(config)# **crypto ipsec transform-set 12b esp-sha-hmac ah-sha-hmac esp-aes 128**

输入“变换集”命令后,会进入其子命令模式,此时可以输入如下命令来定义 IPSec 对等体的工作模式。

mode transport | **tunnel**

使用关键字 transport 将定义该 IPSec SA 使用传输模式,使用关键字 tunnel 则将定义该 IPSec SA 使用隧道模式。

4. 定义受 VPN 保护的流量

在使用访问控制列表定义受 VPN 保护的地址范围时,ACL 中 permit 的 IP 报文会受到 VPN 保护。

注意:一旦定义了某部分流量受到 VPN 保护,则当本地对等体从远端收到没有受到 VPN 保护的这部分流量时,就会将其丢弃,所以需谨慎配置。

例如,在模拟分公司 1 边界路由器和分支机构 B-1 边界路由器上配置站到站 VPN 时,如果要求所有模拟分公司 1 网络 200.100.12.0/24 与分支机构 B-1 网络 200.100.15.0/26 间的所有通信都经站到站 IPSec VPN 保护,则可如下配置对等体上受保护的流量。

(1) 在分公司 1 边界路由器上配置保护流量的 ACL。

R0(config)# **ip access-list extended eacl-vpn-12b**
R0 (config-ext-nacl)# **permit ip 200.100.12.0 0.0.0.255 200.100.15.0 0.0.0.63**

(2) 在分支机构 B-1 边界路由器上配置保护流量的 ACL。

R1(config)# **ip access-list extended eacl-vpn-b21**
R1 (config-ext-nacl)# **permit ip 200.100.15.0 0.0.0.63 200.100.12.0 0.0.0.255**

如上所示,两个边界路由器上配置的 ACL 是对称的。

在分支机构 B-1 内部使用了地址转换时,注意一定要使用 ESP 而不是 AH 协议作为 VPN 隧道的封装协议。由于地址转换会改变 IP 报头,而 AH 协议要求对整个报文进行验证,所以如果地址转换发生在 AH 产生验证前的情况下,会出现校验错误。

5. 定义加密图

在 Cisco IOS 路由器上,定义加密图的操作是在全局配置模式下输入:

```
crypto map 加密图名 加密图条目序号 ipsec-isakmp | ipsec-manual
```

该命令将创建一个指定名称的加密图,并进入指定加密图条目的子命令配置模式。

参数"加密图名"用于指定加密图在网络设备上的唯一标识。

参数"加密图条目序号"用于指定当前对哪条加密图条目进行编辑,编号范围为 1~65535。

关键字 ipsec-isakmp 用于指定该加密图条目是由 ISAKMP/IKE 自动协商的。在该加密图条目没有将对等体和被 VPN 保护的流量范围绑定在一起时,该加密图条目不会生效。

关键字 ipsec-manual 用于指定该加密图条目是手工形成的。

Cisco IOS 路由器的一个接口上只能应用一个加密图,当需要在一个接口上建立多个 VPN 安全隧道时,需要通过在一个加密图中定义多个加密图条目实现。注意,加密图条目的顺序很重要,序号越小,优先级越高。

一旦进入加密图条目子命令配置模式,需要输入以下命令来将前面所定义的 IPSec SA 和被保护流量绑定在一起。

```
set peer IP 地址 | 主机名
set transform-set 变换集名
match address ACL 名 | ACL 号
```

set peer 子命令用于配置远端对等体地址。

set transform-set 子命令用于指定该加密图条目绑定哪个变换集。

match address 子命令用于指定该加密图条目保护哪个 ACL 定义的流量。

例如,在模拟分公司 1 边界路由器上配置到分支机构 B-1 站到站 VPN 时,如果如前配置了变换集名为 12b,ACL 名为 eacl-vpn-12b,分支机构 B-1 对等体 IP 地址为 200.100.15.205,则在分公司 1 上创建相应加密图条目的操作为:

```
VPN-Ser(config)#crypto map 12b 100 ipsec-isakmp
VPN-Ser(config-crypto-map)#set peer 200.100.15.205
VPN-Ser(config-crypto-map)#set transform-set 12b
VPN-Ser(config-crypto-map)#match address eacl-vpn-12b
```

6. 将加密图应用到接口上

加密图只有应用在接口上才能生效。加密图应配置在作为 IPSec VPN 隧道端点的接口上,一般为边界路由器连接外部网络的接口。加密图应用时,不用指定方向。

在 Cisco IOS 路由器上，将加密图应用到接口的操作是在接口配置模式下输入：

crypto map 加密图名

一旦将某个加密图应用在路由器某接口上，路由器会显示如下所示提示信息，提示已经打开了 ISAKMP 进行协商。

```
* Mar 1 03:14:49.371: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

7. 检查 VPN 配置

在 Cisco IOS 路由器上完成 VPN 的配置后，进入特权配置模式下，使用如下命令可以检查有关 ISAKMP SA、IPSec SA 的参数以及加密图的配置应用是否正确。

```
show crypto isakmp policy
show crypto ipsec transform-set
show crypto map
```

例如，使用 show crypto isakmp policy 命令的操作及显示结果如下所示。

```
r0# show crypto isakmp policy

Global IKE policy
Protection suite of priority 1                                              ①
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
        hash algorithm:          Message Digest 5
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                86400 seconds, no volume limit
Default protection suite                                                    ②
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                86400 seconds, no volume limit
```

其中：

① 显示了一个优先级为 1 的 ISAKMP/IKE 策略内容，该策略各项参数含义如表 5-6 所示。

② 显示了系统默认 ISAKMP/IKE 策略内容。

表 5-6 ISAKMP/IKE 策略示例

参 数	参数值	参 数	参数值
加密算法 encryption algorithm	DES	D-H 算法组 Diffie-Hellman group	1
散列算法 hash algorithm	MD5	SA 生存时间	86400
认证方式 authentication method	预共享密钥		

又如，使用 show crypto ipsec transform-set 命令的操作及显示结果如下。

```
r0#show crypto ipsec transform-set
Transform set myvpn: { esp-des }
   will negotiate = { Tunnel, },
```

该结果显示，目前网络设备上配置了一个名为 myvpn 的变换集，该变换集定义 VPN 安全隧道使用 ESP 作为封装协议，对通信数据使用 DES 算法进行加密处理，但不进行认证处理。此安全隧道的工作模式为隧道模式。

再如，使用 show crypto map 命令的操作及输出结果如下。

```
r0#show crypto map
Crypto Map "myvpn" 100 ipsec-isakmp
        Peer = 200.100.10.254
        Extended IP access list eacl-vpn
            access-list eacl-vpn permit ip 172.16.16.0 0.0.0.255 192.168.0.0 0.0.0.255
        Current peer: 200.100.10.254
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                myvpn,
        }
        Interfaces using crypto map myvpn:
                FastEthernet0/0
```

该输出结果显示，在网络设备上已配置了一个名为 myvpn 的加密图；该加密图绑定的远端对等体 IP 地址为 200.100.10.254，所保护的流量由一个名为 eacl-vpn 的扩展 ACL 定义；该 ACL 允许本地网络 172.16.16.0/24 到远端网络 192.168.0.0/24 的流量将受到 myvpn 的保护；该加密图绑定的变换集名为 myvpn；该加密图被应用到接口 FastEthernet0/0 上。

8. 检查 VPN 状态信息

除了可以使用以上 3 条命令检查配置外，还可以在特权模式下，使用如下命令检查对等体上已建立的 ISAKMP SA 和 IPSec SA 的状态信息。

```
show crypto isakmp sa
show crypto ipsec sa
```

例如，检查已建立的 ISAKMP SA 状态信息的操作及输出结果如下。

```
r0#show crypto isakmp sa
dst             src             state       conn-id     slot
200.100.10.254  200.100.10.1    QM_IDLE     1           0
```

该信息显示已经在远端 200.100.10.254 和本地 200.100.10.1 建立一个 ISAKMP SA，其目前状态为 QM_IDLE，其连接 ID 号为 1。利用连接 ID 号可以在检查过程中删除已建立 SA 时使用。

又如，检查已建立的 IPSec SA 状态信息的操作及输出结果如下。

```
r0#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: myvpn, local addr. 200.100.10.1                                  ①

protected vrf:
   local  ident (addr/mask/prot/port): (172.16.16.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
   current_peer: 200.100.10.254:500                                                  ②
      permit, flags={origin_is_acl,}                                                 ③
   #pkts encaps: 18, #pkts encrypt: 18, #pkts digest 0
   #pkts decaps: 18, #pkts decrypt: 18, #pkts verify 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 2, #recv errors 0

      local crypto endpt.: 200.100.10.1, remote crypto endpt.: 200.100.10.254       ④
      path mtu 1500, ip mtu 1500
      current outbound spi: DE35F95F                                                 ⑤

      inbound esp sas:                                                               ⑥
       spi: 0xA2E86721(2733139745)                                                   ⑦
         transform: esp-des ,                                                        ⑧
         in use settings ={Tunnel, }                                                 ⑨
         slot: 0, conn id: 2000, flow_id: 1, crypto map: myvpn                       ⑩
         sa timing: remaining key lifetime (k/sec): (4586045/3221)                   ⑪
         IV size: 8 bytes
         replay detection support: N

         inbound ah sas:                                                             ⑫

         inbound pcp sas:                                                            ⑬

         outbound esp sas:
          spi: 0xDE35F95F(3728079199)                                                ⑭
            transform: esp-des ,
            in use settings ={Tunnel, }
            slot: 0, conn id: 2001, flow_id: 2, crypto map: myvpn
            sa timing: remaining key lifetime (k/sec): (4586045/3221)
            IV size: 8 bytes
            replay detection support: N

         outbound ah sas:                                                            ⑮

         outbound pcp sas:                                                           ⑯
```

以上输出结果说明如下。

① 目前在接口 FastEthernet0/0 上应用了一个名为 myvpn 的加密图。该接口的 IP 地址为 200.100.10.1。

② 当前 IPSec SA 连接的远端对等体 IP 地址为 200.100.10.254，端口 500。

③ 当前 IPSec SA 保护的流量是由 ACL 中 permit 语句定义的。接下来显示了各有 18 个匹配 ACL 的数据报文被进行了封装/解封装处理；并且这些数据报文都被进行了加/解密处理，但没有被进行认证处理。

④ 此处输出结果显示，该 IPSec SA 的本端对等体为 200.100.10.1，远端对等体为 200.100.10.254。

⑤ 此处输出结果显示在当前对等体上出站流量中的 SPI 值为 DE35F95F。

⑥ 此处显示当前在入站方向上有已建立的 IPSec SA，其类型为 ESP SA。

⑦ 该入站 ESP SA 使用的 SPI 值为 0xA2E86721。

⑧ 该入站 ESP SA 使用的变换集为 ESP-DES，即使用 ESP 协议进行封装，并对数据使用 DES 算法进行加密。

⑨ 该入站 ESP SA 使用的工作模式是隧道模式。

⑩ 该入站 ESP SA 使用的加密图名为 myvpn。

⑪ 该入站 ESP SA 的生存时间。

⑫ 入站方向上没有建立 AH 协议封装的 SA。

⑬ 入站方向上没有建立 PCP SA。

⑭ 出站方向上有已建立的 IPSec SA，该 SA 使用 ESP 协议封装，其各项参数含义与入站方向上的相同。

⑮ 出站方向上没有建立 AH 协议封装的 SA。

⑯ 出站方向上没有建立 PCP SA。

9. 跟踪检查 ISAKMP SA、IPSec SA 建立过程

当使用检查配置、状态命令都无法检查出 VPN 错误时，在 Cisco IOS 路由器上，还可以通过跟踪命令，跟踪 ISAKMP SA、IPSec SA 建立过程，以发现错误。

在 Cisco IOS 路由器上，跟踪 ISAKMP SA 建立过程的命令为：

debug　crypto　isakmp

在 Cisco IOS 路由器上，跟踪 IPSec SA 建立过程的命令为：

debug　crypto　ipsec

例如，跟踪 ISAKMP SA 建立过程的操作及输出结果如下。

```
r0#debug  crypto  isakmp
Crypto ISAKMP debugging is on
r0#
*Mar  1 05:55:52.706: ISAKMP (0:0): received packet from 200.100.10.254 dport 500 sport
500 Global (N) NEW SA                                                              ①
*Mar  1 05:55:52.710: ISAKMP: local port 500, remote port 500
*Mar  1 05:55:52.710: ISAKMP: insert sa successfully sa = 6400FCD0
```

```
* Mar  1 05:55:52.714: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
* Mar  1 05:55:52.714: ISAKMP (0:1): Old State = IKE_READY  New State = IKE_R_MM1
* Mar  1 05:55:52.714: ISAKMP (0:1): processing SA payload. message ID = 0
* Mar  1 05:55:52.718: ISAKMP (0:1): processing vendor id payload
* Mar  1 05:55:52.718: ISAKMP (0:1): vendor ID seems Unity/DPD but major 157 mismatch
* Mar  1 05:55:52.718: ISAKMP (0:1): vendor ID is NAT-T v3
* Mar  1 05:55:52.718: ISAKMP (0:1): processing vendor id payload
* Mar  1 05:55:52.718: ISAKMP (0:1): vendor ID seems Unity/DPD but major 123 mismatch
* Mar  1 05:55:52.718: ISAKMP (0:1): vendor ID is NAT-T v2
* Mar  1 05:55:52.718: ISAKMP: Looking for a matching key for 200.100.10.254 in default :
success                                                                        ②
* Mar  1 05:55:52.722: ISAKMP (0:1): found peer pre-shared key matching 200.100.10.254
* Mar  1 05:55:52.722: ISAKMP (0:1) local preshared key found
* Mar  1 05:55:52.722: ISAKMP : Scanning profiles for xauth ...
* Mar  1 05:55:52.722: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1
policy                                                                         ③
* Mar  1 05:55:52.722: ISAKMP:      encryption DES-CBC
* Mar  1 05:55:52.722: ISAKMP:      hash MD5
* Mar  1 05:55:52.722: ISAKMP:      default group 1
* Mar  1 05:55:52.722: ISAKMP:      auth pre-share
* Mar  1 05:55:52.726: ISAKMP:      life type in seconds
* Mar  1 05:55:52.726: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
* Mar  1 05:55:52.726: ISAKMP (0:1): atts are acceptable. Next payload is 0
* Mar  1 05:55:52.778: ISAKMP (0:1): processing vendor id payload
* Mar  1 05:55:52.778: ISAKMP (0:1): vendor ID seems Unity/DPD but major 157 mismatch
* Mar  1 05:55:52.778: ISAKMP (0:1): vendor ID is NAT-T v3
* Mar  1 05:55:52.778: ISAKMP (0:1): processing vendor id payload
* Mar  1 05:55:52.782: ISAKMP (0:1): vendor ID seems Unity/DPD but major 123 mismatch
* Mar  1 05:55:52.782: ISAKMP (0:1): vendor ID is NAT-T v2
* Mar  1 05:55:52.782: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_
MAIN_MODE
* Mar  1 05:55:52.782: ISAKMP (0:1): Old State = IKE_R_MM1  New State = IKE_R_MM1
* Mar  1 05:55:52.786: ISAKMP (0:1): constructed NAT-T vendor-03 ID
* Mar  1 05:55:52.786: ISAKMP (0:1): sending packet to 200.100.10.254 my_port 500 peer_
port 500 (R) MM_SA_SETUP                                                       ④
* Mar  1 05:55:52.786: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_
COMPLETE
* Mar  1 05:55:52.790: ISAKMP (0:1): Old State = IKE_R_MM1  New State = IKE_R_MM2
* Mar  1 05:55:53.302: ISAKMP (0:1): received packet from 200.100.10.254 dport 500 sport
500 Global (R) MM_SA_SETUP
* Mar  1 05:55:53.306: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
* Mar  1 05:55:53.306: ISAKMP (0:1): Old State = IKE_R_MM2  New State = IKE_R_MM3
* Mar  1 05:55:53.306: ISAKMP (0:1): processing KE payload. message ID = 0
* Mar  1 05:55:53.366: ISAKMP (0:1): processing NONCE payload. message ID = 0
* Mar  1 05:55:53.366: ISAKMP: Looking for a matching key for 200.100.10.254 in default : success
* Mar  1 05:55:53.366: ISAKMP (0:1): found peer pre-shared key matching 200.100.10.254
```

```
* Mar  1 05:55:53.370: ISAKMP (0:1): SKEYID state generated
* Mar  1 05:55:53.370: ISAKMP (0:1): processing vendor id payload
* Mar  1 05:55:53.370: ISAKMP (0:1): vendor ID is Unity
* Mar  1 05:55:53.370: ISAKMP (0:1): processing vendor id payload
* Mar  1 05:55:53.374: ISAKMP (0:1): vendor ID is DPD
* Mar  1 05:55:53.374: ISAKMP (0:1): processing vendor id payload
* Mar  1 05:55:53.374: ISAKMP (0:1): speaking to another IOS box!
* Mar  1 05:55:53.374: ISAKMP:received payload type 17
* Mar  1 05:55:53.374: ISAKMP:received payload type 17
* Mar  1 05:55:53.374: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_
MAIN_MODE
* Mar  1 05:55:53.378: ISAKMP (0:1): Old State = IKE_R_MM3   New State = IKE_R_MM3
* Mar  1 05:55:53.378: ISAKMP (0:1): sending packet to 200.100.10.254 my_port 500 peer_
port 500 (R) MM_KEY_EXCH
* Mar  1 05:55:53.382: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_
COMPLETE
* Mar  1 05:55:53.382: ISAKMP (0:1): Old State = IKE_R_MM3   New State = IKE_R_MM4
* Mar  1 05:55:53.738: ISAKMP (0:1): received packet from 200.100.10.254 dport 500 sport
500 Global (R) MM_KEY_EXCH
* Mar  1 05:55:53.742: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
* Mar  1 05:55:53.742: ISAKMP (0:1): Old State = IKE_R_MM4   New State = IKE_R_MM5
* Mar  1 05:55:53.746: ISAKMP (0:1): processing ID payload. message ID = 0
* Mar  1 05:55:53.746: ISAKMP (0:1): ID payload                                  ⑤
          next-payload : 8
          type         : 1
          address      : 200.100.10.254
          protocol     : 17
          port         : 500
          length       : 12
* Mar  1 05:55:53.746: ISAKMP (0:1): peer matches *none* of the profiles
* Mar  1 05:55:53.746: ISAKMP (0:1): processing HASH payload. message ID = 0
* Mar  1 05:55:53.750: ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 6400FCD0
* Mar  1 05:55:53.750: ISAKMP (0:1): SA authentication status:
* Mar  1 05:55:53.750:   authenticated
* Mar  1 05:55:53.750: ISAKMP (0:1): Process initial contact,
bring down existing phase 1 and 2 SA's with local 200.100.10.1 remote 200.100.10.254 remote
port 500
* Mar  1 05:55:53.750: ISAKMP (0:1): SA authentication status:                   ⑥
* Mar  1 05:55:53.750:   authenticated
* Mar  1 05:55:53.754: ISAKMP (0:1): SA has been authenticated with 200.100.10.254
* Mar  1 05:55:53.754: ISAKMP (0:1): peer matches *none* of the profiles
* Mar  1 05:55:53.754: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_
MAIN_MODE
* Mar  1 05:55:53.754: ISAKMP (0:1): Old State = IKE_R_MM5   New State = IKE_R_MM5
* Mar  1 05:55:53.758: ISAKMP (0:1): SA is doing pre-shared key authentication using id type
```

```
ID_IPv4_ADDR
* Mar  1 05:55:53.758: ISAKMP (0:1): ID payload
        next-payload : 8
        type         : 1
        address      : 200.100.10.1
        protocol     : 17
        port         : 500
        length       : 12
* Mar  1 05:55:53.758: ISAKMP (1): Total payload length: 12
* Mar  1 05:55:53.762: ISAKMP (0:1): sending packet to 200.100.10.254 my_port 500 peer_
port 500 (R) MM_KEY_EXCH
* Mar  1 05:55:53.762: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_
COMPLETE
* Mar  1 05:55:53.762: ISAKMP (0:1): Old State = IKE_R_MM5  New State = IKE_P1_
COMPLETE
* Mar  1 05:55:53.766: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PHASE1_
COMPLETE
* Mar  1 05:55:53.766: ISAKMP (0:1): Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
* Mar  1 05:55:54.054: ISAKMP (0:1): received packet from 200.100.10.254 dport 500 sport
500 Global (R) QM_IDLE
* Mar  1 05:55:54.058: ISAKMP: set new node 2037258125 to QM_IDLE          ⑦
* Mar  1 05:55:54.058: ISAKMP (0:1): processing HASH payload. message ID = 2037258125
* Mar  1 05:55:54.058: ISAKMP (0:1): processing SA payload. message ID = 2037258125 ⑧
* Mar  1 05:55:54.062: ISAKMP (0:1): Checking IPSec proposal 1
* Mar  1 05:55:54.062: ISAKMP: transform 1, ESP_DES
* Mar  1 05:55:54.062: ISAKMP:   attributes in transform:
* Mar  1 05:55:54.062: ISAKMP:      encaps is 1 (Tunnel)
* Mar  1 05:55:54.062: ISAKMP:      SA life type in seconds
* Mar  1 05:55:54.062: ISAKMP:      SA life duration (basic) of 3600
* Mar  1 05:55:54.062: ISAKMP:      SA life type in kilobytes
* Mar  1 05:55:54.062: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
* Mar  1 05:55:54.066: ISAKMP (0:1): atts are acceptable.
* Mar  1 05:55:54.066: ISAKMP (0:1): processing NONCE payload. message ID = 2037258125
* Mar  1 05:55:54.070: ISAKMP (0:1): processing ID payload. message ID = 2037258125
* Mar  1 05:55:54.070: ISAKMP (0:1): processing ID payload. message ID = 2037258125
* Mar  1 05:55:54.070: ISAKMP (0:1): asking for 1 spis from ipsec
* Mar  1 05:55:54.070: ISAKMP (0:1): Node 2037258125, Input = IKE_MESG_FROM_
PEER, IKE_QM_EXCH
* Mar  1 05:55:54.070: ISAKMP (0:1): Old State = IKE_QM_READY  New State = IKE_
QM_SPI_STARVE
* Mar  1 05:55:54.074: ISAKMP: received ke message (2/1)
* Mar  1 05:55:54.322: ISAKMP (0:1): sending packet to 200.100.10.254 my_port 500 peer_
port 500 (R) QM_IDLE
* Mar  1 05:55:54.326: ISAKMP (0:1): Node 2037258125, Input = IKE_MESG_FROM_
IPSEC, IKE_SPI_REPLY
```

```
*Mar  1 05:55:54.326: ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE  New State =
IKE_QM_R_QM2
*Mar  1 05:55:54.462: ISAKMP (0:1): received packet from 200.100.10.254 dport 500 sport
500 Global (R) QM_IDLE
*Mar  1 05:55:54.470: ISAKMP (0:1): Creating IPSec SAs                            ⑨
*Mar  1 05:55:54.470:        inbound SA from 200.100.10.254 to 200.100.10.1 (f/i)
0/ 0 (proxy 192.168.0.0 to 172.16.16.0)
*Mar  1 05:55:54.470:        has spi 0x74788662 and conn_id 2000 and flags 2
*Mar  1 05:55:54.470:        lifetime of 3600 seconds
*Mar  1 05:55:54.474:        lifetime of 4608000 kilobytes
*Mar  1 05:55:54.474:        has client flags 0x0
*Mar  1 05:55:54.474:        outbound SA from 200.100.10.1  to 200.100.10.254  (f/i)
0/ 0 (proxy 172.16.16.0  to 192.168.0.0)
*Mar  1 05:55:54.474:        has spi -656764648 and conn_id 2001 and flags A
*Mar  1 05:55:54.474:        lifetime of 3600 seconds
*Mar  1 05:55:54.474:        lifetime of 4608000 kilobytes
*Mar  1 05:55:54.474:        has client flags 0x0
*Mar  1 05:55:54.478: ISAKMP (0:1): deleting node 2037258125 error FALSE reason "quick
mode done (await)"
*Mar  1 05:55:54.478: ISAKMP (0:1): Node 2037258125, Input = IKE_MESG_FROM_
PEER, IKE_QM_EXCH
*Mar  1 05:55:54.478: ISAKMP (0:1): Old State = IKE_QM_R_QM2  New State = IKE_
QM_PHASE2_COMPLETE
```

以上输出结果说明如下。

① 路由器在接口收到的流量与需要受保护的 ACL 相匹配,所以路由器被触发建立 ISAKMP SA。

② 路由器成功找到与远端对等体 200.100.10.254 建立安全关联所需的密钥。

③ 路由器找到所配置的 ISAKMP/IKE 策略 1。

④ 对等体间开始发送 IKE 报文,尝试建立 ISAKMP SA。

⑤ 对等体间使用 ISAKMP 进行协商。ISAKMP 使用 UDP 500 进行通信。

⑥ 对等体间通过认证。

⑦ ISAKMP SA 建立成功。

⑧ 在 ISAKMP SA 上交换建立 IPSec SA 的信息。

⑨ 成功建立 IPSec SA。

又如,跟踪 IPSec SA 的操作及输出结果如下。

```
r0#debug  crypto  ipsec
Crypto IPSEC debugging is on
*Mar  1 06:13:19.718: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has
invalid spi for                                                                   ①
      destaddr=200.100.10.1,prot=50,spi=0x74788662(1954055778),srcaddr=200.100.10.254
*Mar  1 06:13:21.718: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 200.100.10.1, remote= 200.100.10.254,
    local_proxy= 172.16.16.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.0.0/255.255.255.0/0/0 (type=4),
```

```
    protocol= ESP, transform= esp-des  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
* Mar  1 06:13:21.722: IPSEC(kei_proxy): head = myvpn, map->ivrf = , kei->ivrf =
* Mar  1 06:13:21.726: IPSEC(key_engine): got a queue event...
* Mar  1 06:13:21.726: IPSEC(spi_response): getting spi 2226639570 for SA        ②
        from 200.100.10.1     to 200.100.10.254   for prot 3
* Mar  1 06:13:22.098: IPSEC(key_engine): got a queue event...
* Mar  1 06:13:22.098: IPSEC(initialize_sas): ,                                  ③
  (key eng. msg.) INBOUND local= 200.100.10.1, remote= 200.100.10.254,
    local_proxy= 172.16.16.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.0.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0x84B7D2D2(2226639570), conn_id= 2000, keysize= 0, flags= 0x2
* Mar  1 06:13:22.102: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 200.100.10.1, remote= 200.100.10.254,
    local_proxy= 172.16.16.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.0.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0xB5CC379E(3050059678), conn_id= 2001, keysize= 0, flags= 0xA
* Mar  1 06:13:22.102: IPSEC(kei_proxy): head = myvpn, map->ivrf = , kei->ivrf =
* Mar  1 06:13:22.106: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same
proxies and 200.100.10.254
* Mar  1 06:13:22.106: IPSEC(add mtree): src 172.16.16.0, dest 192.168.0.0, dest_port 0

* Mar  1 06:13:22.106: IPSEC(create_sa): sa created,                             ④
  (sa) sa_dest= 200.100.10.1, sa_prot= 50,
    sa_spi= 0x84B7D2D2(2226639570),
    sa_trans= esp-des , sa_conn_id= 2000
* Mar  1 06:13:22.110: IPSEC(create_sa): sa created,
  (sa) sa_dest= 200.100.10.254, sa_prot= 50,
    sa_spi= 0xB5CC379E(3050059678),
    sa_trans= esp-des , sa_conn_id= 2001
```

显示内容说明如下。

① 对等体收到了一个错误 SPI 的 SA。

② 对等体重新建立 IPSec SA，并向远端对等体发送新 SPI。

③ 对等体间开始初始化新的 IPSec SA。

④ 对等体间建立新的 IPSec SA。

10. 清除已存在的 SA

进行调试时，有时需要清除已建立的 SA，以查看修改 VPN 配置后的效果。在 Cisco IOS 路由器上清除已建立的 SA 的操作为，在特权模式下输入：

clear crypto sa map 加密图名

5.3.2 远程访问 VPN 配置

远程访问 VPN 有两种实现方法：远程 IPSec VPN 和 SSL VPN。

在 Cisco 网络设备上，远程 IPSec VPN 又有两种实现方案：Easy VPN 和动态 VTI (DVTI)。

Easy VPN 的架构包括两部分：①在网络设备上的远程访问 VPN 服务器；②Cisco Easy VPN Remote，如在远程用户计算机上的 Cisco VPN 客户端软件、Easy VPN 硬件客户端或在网络设备上配置的 Easy VPN 客户端。

Easy VPN 将大量 VPN 通信的管理工作，如定义大量 VPN 通信参数、对远端 VPN 对等体进行失效检查等，集中在 VPN 服务器一端进行。因此与站到站 VPN 不同，实施 Easy VPN 时，VPN 服务器和 VPN 客户端的配置操作有很大区别。

1. Easy VPN 服务器配置

与站到站 VPN 相比，Easy VPN 为简化在客户端的配置，除提供建立 VPN 安全隧道的基本功能外，还提供以下功能。

- 一旦 VPN 安全通道建立成功，Easy VPN 服务器可以为远程访问用户分配访问公司内部网络的 IP 地址，使其可以像使用专用线路一样访问公司网络，并自动建立 NAT 或 PAT，关联必要的 ACL。
- 对用户身份进行认证，以对其进行访问控制。
- 由 Easy VPN 服务器端将 VPN 安全通道的各项参数作为组策略推送到 VPN 客户端。

Easy VPN 服务器与 Easy VPN 客户端之间对等体的会话步骤如下。

① 使用 ISAKMP 在 Easy VPN 服务器与 Easy VPN 客户端间进行认证。

② 使用 IKE 扩展认证(IKE Extended Authentication，Xauth)对用户身份进行认证。

③ 通过认证后，VPN 服务器向 VPN 客户端推送组策略。

④ 创建 IPSec SA。

由于以上所述变换，所以在 Easy VPN 服务器一端，除需要进行 ISAKMP 策略、变换集和加密图的定义以及应用加密图等操作外，还需要以下配置操作。

- 增加 IP 地址池等有关配置。
- 增加用户身份认证、授权的配置。
- 增加推送组策略的定义。
- 需要将所定义的身份认证、授权等与加密图绑定在一起。

在 Cisco IOS 路由器上配置 Easy VPN 的基本步骤如表 5-7 所示。

注意：Easy VPN 在配置过程中有如下限制。

- ISAKMP 策略中只支持 group 2。
- 变换集必须既有加密，也有认证，并且不支持 AH。
- Easy VPN 客户端使用分隔隧道(即使用 ACL 限制通过安全隧道的流量)时，不支持 NAT。

表 5-7 Easy VPN 配置基本步骤

序 号	操 作	相 关 命 令	必要
步骤 1	创建 IP 地址池，为远程访问用户分配可本地使用的 IP 地址	**ip local pool**	是
步骤 2	为远程访问用户配置访问网络的 AAA 授权策略	**aaa new-model** **aaa authorization network**	是
步骤 3	定义 ISAKMP 策略	**crypto isakmp policy**	是
步骤 4	创建推送到客户端的组策略	**crypto isakmp client configuration group**	是
步骤 5	创建变换集	**crypto ipsec transform-set**	是
步骤 6	创建动态加密图	**crypto dynamic-map**	是
步骤 7	将动态加密图插入到静态加密图中	**crypto map**	是
步骤 8	修改其他加密图参数	**crypto map map -rvpn client configuration address respond** **crypto map xx isakmp authorization list**	是
步骤 9	将加密图应用到接口上	接口模式下的 **crypto map**	是
步骤 10	启用 IKE 失效对等体检测	**crypto isakmp keepalive**	是
步骤 11	配置 Xauth	**crypto map … client authentication list**	可选
步骤 12	检查 Easy VPN 配置	**show cryto map** **show cryto isakmp client ezvpn**	可选

（1）创建 IP 地址池

在 Cisco IOS 路由器上，创建 IP 地址池的操作为，在全局配置模式下输入：

ip local pool ｛ **default** ｜ 地址池名 地址池最小地址 地址池最大地址｝

例如，在分支机构 B-1 边界路由器上配置远程访问 VPN 时，设计让远程访问用户接入后使用 10.0.4.1～10.0.4.254 间地址，则可以如下配置。

VPN-Ser (config)＃**ip local pool pool-rvpn 10.0.0.？ 10.0.0.？**

（2）为远程访问用户配置 AAA 策略

有关 AAA 策略配置方法，可以参考本书第 3 章有关内容。

注意：对于远程访问 VPN 用户，需为其配置 AAA 网络访问授权。

例如，在分支机构 B-1 边界路由器上配置远程访问 VPN 时，如果设计使用路由器本地数据库进行网络访问授权，并且本地配置相应用户名为 rvpn，口令为 123，则可以如下操作。

VPN-Ser(config)＃**aaa new-model**
VPN-Ser(config)＃**aaa authorization network rvpn local**
VPN-Ser(config)＃**username rvpn password 123**

（3）创建推送到客户端的组策略

在 Cisco IOS 路由器上，创建推送到客户端组策略的操作为，先在全局配置模式下输入：

crypto isakmp client configuration group 策略组号

这时将进入组策略配置模式，可以输入如下子命令定义组策略各项参数。

```
key     预共享密钥
pool    地址池名
dns     DNS 服务器地址
domain  本地域
acl     访问控制列表号或名
```

其中，子命令 key 用于定义 VPN 服务器与客户端对等体间认证的预共享密钥。

子命令 pool 用于定义 VPN 客户端访问时使用的 IP 地址从哪个地址池进行分配。

子命令 dns 用于定义 VPN 客户端远程访问时，使用哪个 DNS 服务器。

子命令 domain 用于定义发送给客户端的默认域名。

子命令 acl 用于定义客户端可以访问本地哪些网络。

例如，在分支机构 B-1 边界路由器上配置远程访问 VPN 时，若设计：使用预共享密钥为 123，地址池为 pool-rvpn，DNS 服务器地址为 120.0.0.29。配置其组策略的操作如下。

```
VPN-Ser(config)#crypto   isakmp   client   configuration   group   rvpn-1
VPN-Ser(config-isakmp-group)#key   123
VPN-Ser(config-isakmp-group)#pool   pool-rvpn
VPN-Ser(config-isakmp-group)#dns   120.0.0.29
```

注意：此处访问控制列表用于定义本地网络中受 VPN 保护的地址范围。

(4) 创建动态加密图

由于 Easy VPN 的客户端一般 IP 地址不固定，所以需创建动态加密图将变换集与被保护的流量绑定在一起。

在 Cisco IOS 路由器上，创建动态加密图的操作为，在全局配置模式下输入：

```
crypto   dynamic-map   动态加密图名   加密图条目序号
set   transform-set   变换集名   [ 变换集名 ... ]
reverse-route
```

参数"动态加密图名"、"加密图条目序号"的用法与配置静态加密图相同。

在创建加密图条目并进入其配置模式后，需使用 set transform-set 子命令指定动态加密图绑定的变换集，可以指定多个变换集，但排在左边的优先。

如果要保证 IPSec 隧道的返回数据能够找到该隧道，还需要输入 reverse-route 子命令，让路由器为每个 VPN 客户端的内部 IP 地址在 Easy VPN 服务器上创建一条静态路由。

例如，以下操作将创建一个名为 dmap-rvpn 的动态加密图，并创建一个序号为 100 的加密图条目，在该加密图条目中绑定了变换集 dts-rvpn，同时启用了反向路由功能。

```
VPN-Ser(config)#crypto   dynamic-map   dmap-rvpn   100
VPN-Ser(config-crypto-map)#set   transform-set   dts-rvpn
VPN-Ser(config-crypto-map)#reverse-route
```

(5) 配置加密图

在 Cisco 网络设备上，动态加密图不能直接应用在接口上，还需配置静态加密图，然后将动态加密图插入到该静态加密图中。

在 Cisco IOS 路由器上，将动态加密图插入到静态加密图的操作为在全局配置模式下输入：

crypto map 加密图名 加密图条目 **ipsec-isakmp dynamic** 动态加密图条目

例如，将一个名为 dmp-rvpn 的动态加密图插入到 map-rvpn 中第 10 行的操作如下。

VPN-Ser(config)# **crypto map map-rvpn 10 ipsec-isakmp dynamic dmap-rvpn**

(6) 配置 VPN 服务器响应 VPN 客户端请求并为其授权的方案

对于 Cisco IOS 路由器而言，还需要输入如下命令使 Easy VPN 服务器能够响应客户端的请求。

crypto map 加密图名 **client configuration address respond**

另外，当用户发起远程访问时，应定义路由器使用什么样的授权策略。

crypto map 加密图名 **isakmp authorization list** AAA 授权策略名

例如，如下操作将一个名为 rvpn 的授权策略与名为 map-rvpn 的加密图绑定在一起，则远程用户访问时，将受到该授权策略的限制。

VPN-Ser(config)# **crypto map map-rvpn isakmp authorization list rvpn**

(7) 启用 IKE 失效对等体检测

路由器使用失效对等体检测(Dead Peer Detection，DPD)，可以检测远端对等体是否依然存活。Cisco 路由器提供两种 DPD 机制：按需 DPD(on-demand DPD)和定期 DPD(periodic DPD)。按需 DPD 是 Cisco 路由器默认配置。

当使用按需 DPD 机制时，路由器根据是否有出站流量发送 DPD 消息。

当配置了 IKE 失效对等体生存时间时，路由器会根据指定的时间间隔发送 Hello 消息。如果路由器未在指定时间间隔收到远端对等体的 Hello 消息，则认为远端对等体已经失效。

在 Cisco IOS 路由器上，启用 IKE 失效对等体检测的操作为在全局配置模式下输入：

crypto isakmp keepalive 生存时间

参数“生存时间”为多长时间进行失效检测，单位为秒，范围为 10～3600。

(8) 配置 Xauth

在 Cisco IOS 路由器上，配置进行登录身份认证的操作为在全局配置模式下输入：

crypto map 加密图名 **client authentication list** AAA 身份认证策略名

当然 AAA 身份认证策略应已经定义，如果使用本地认证，则相应的用户名、口令也应提前配置。

2. Easy VPN 客户端配置

使用 Cisco VPN 客户端软件，可以帮助用户连接到 Easy VPN 服务器，建立 IPSec VPN 安全隧道。

图 5-21 为该软件主窗口。使用该软件的步骤如下。

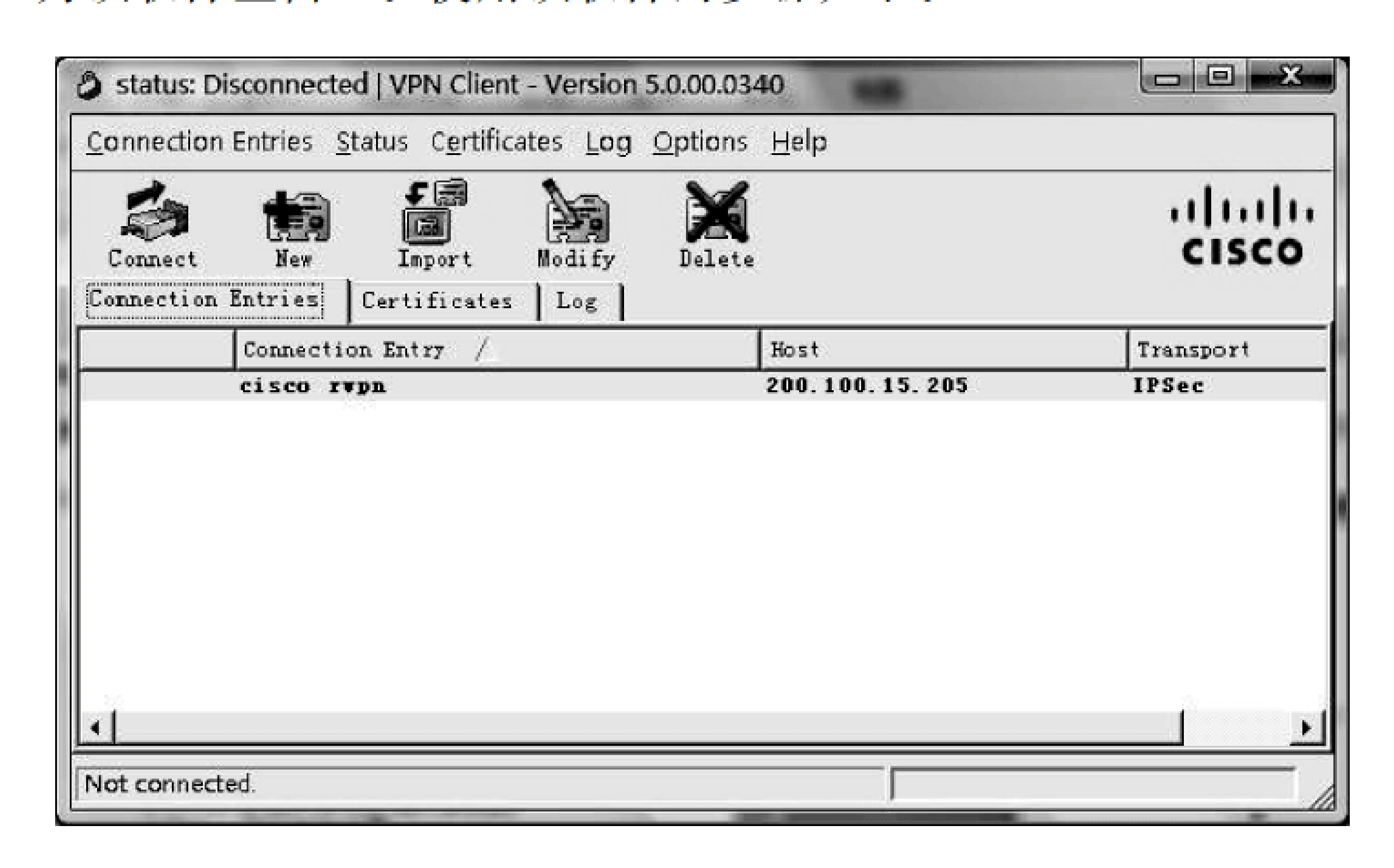


图 5-21 Cisco VPN 客户端软件主窗口

（1）创建 VPN 连接配置项并定义连接参数

在主窗口中单击图标，新建一个连接配置。在出现图 5-22 所示的窗口中，输入 VPN 连接所需参数。

图 5-22 新建 VPN 连接配置窗口

在图 5-22 所示的窗口中，建立预共享密钥方式 VPN 连接所需的必要参数有：VPN 服务器地址 Host、组策略名 Name、组策略预共享密钥 Password 和 Confirm Password。

例如，如果 Easy VPN 服务器的 IP 为 200.100.15.205，在 Easy VPN 服务器上为远程访问用户配置了组策略 rvpn-1，组策略预共享密钥为 123，则可以设置 Host 为 200.100.15.205，Name 为 rvpn-1，Password 和 Confirm Password 为 123。

配置完成后，单击 Save 按钮保存，则在主窗口中会出现新定义的 VPN 连接项记录。

(2) 建立 VPN 连接

在保证运行该客户端软件的计算机已能连接到 Internet 的情况下,选择 Cisco VPN 客户端软件窗口中已经配置好的 VPN 连接项,然后单击窗口上方的 Connect 图标,连接 Easy VPN 服务器。

在连接过程中会弹出一个状态窗口,显示连接状态信息,如图 5-23 所示。

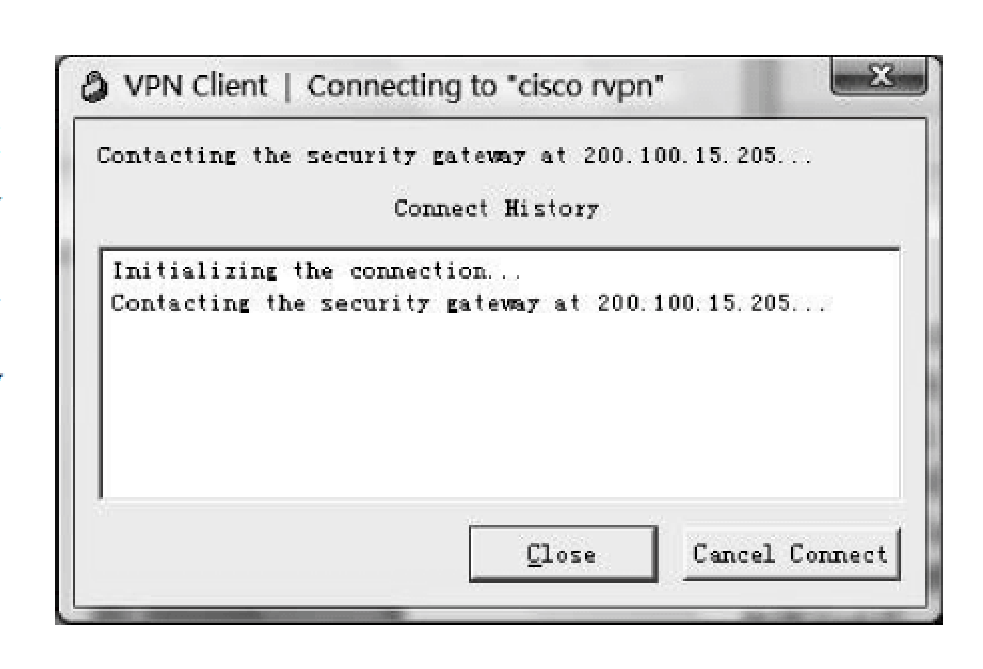


图 5-23 VPN 连接状态信息窗口

在建立连接过程中,如果协商 ISAKMP 策略通过,则 Cisco VPN 客户端软件会弹出如图 5-24 所示窗口,让用户输入账户名和口令。在该窗口中输入在 Easy VPN 服务器上配置的用户账户及口令,单击 OK 按钮,发送账户信息。

如果通过身份认证,并且能够在客户端与服务器成功协商建立 IPSec SA,则 Cisco VPN 客户端软件会提示已经成功建立 VPN 安全隧道,如图 5-25 所示。单击 OK 按钮,关闭窗口即可。



图 5-24 用户登录认证窗口



图 5-25 VPN 连接建立成功窗口

5.4 模拟公司网络安全通信配置方案

根据 5.1 节模拟公司网络安全通信需求,可在分支机构 B-1 边界路由器上进行如下配置。

- 站到站 VPN,其各项参数如表 5-8 所示。
- Easy VPN 服务器,其主要配置参数如表 5-9 所示。

表 5-8 站到站 VPN 配置参数

ISAKMP 策略	变换集参数	加密图参数
优先级:1 加密算法:3DES 散列算法:SHA D-H 算法:2 认证方式:预共享密钥 预共享密钥:随机生成	变换集名:ts-vpn-公司机构代号 封装协议及加密算法:ESP-3DES 封装协议及认证算法:ESP-SHA-HMAC	加密图名:map-vpn 加密图条目序号:公司机构代号

表中“公司机构代号”为公司所有机构网络的数字编号。分支机构与公司其他网络对等体间预共享密钥使用随机算法生成，每月更换。

表 5-9 远程访问 VPN 配置参数

ISAKMP 策略	变换集参数	加密图参数
优先级：1 加密算法：3DES 散列算法：SHA D-H 算法：2 认证方式：预共享密钥 预共享密钥：随机生成	变换集名：ts-rvpn 封装协议及加密算法：ESP-3DES 封装协议及认证算法：ESP-SHA-HMAC	加密图名：map-vpn 动态加密图名：dmap-rvpn 加密图条目序号：100

表中分别使用 ts-rvpn 作为变换集名、动态加密图名。

5.5 小结

使用 VPN 技术可以对通信数据进行加密、验证，保证网络通信的安全可靠性。VPN 技术分为站到站 VPN 和远程访问 VPN 两大类。基于 IPSec 协议框架构建的 VPN，其安全隧道建立过程分为两个阶段。第 1 个阶段协商建立用于传输 VPN 管理信息的 ISAKMP SA，第 2 个阶段建立用于传输通信数据的 IPSec SA。站到站 IPSec VPN 的基本配置步骤包括：①定义 ISAKMP 策略集；②定义 IPSec 变换集；③定义加密图；④应用加密图。Easy VPN 的基本配置步骤包括：①定义用户身份认证；②定义 ISAKMP 策略集；③定义组策略；④定义 IPSec 变换集；⑤定义动态加密图，并将动态加密图插入到静态加密图；⑥应用加密图。

5.6 习题

1. 网络管理员发现路由器 A 不能与路由器 B 建立站到站 VPN 连接，并且在路由器 A 上使用 debug 命令根本检查不到任何协商建立 ISAKMP SA 过程的信息，则以下哪些原因是可能的？（　　）

A. 没有在正确接口上应用加密图
B. 配置了错误的远端对等体地址
C. 加密图名字中使用了数字
D. 接口上配置的 ACL 过滤了 UDP 500 端口的流量
E. ISAKMP 策略优先级使用了太小的数字

2. 下列哪一项是所有选项中安全性最强的加密、验证算法组合？（　　）

A. DES、3DES　　B. AES、SHA　　C. 3DES、SHA　　D. MD5、AES
E. SHA、DES　　F. AES、DES　　G. 3DES、MD5

3. 判断题：使用传输模式时，隧道中数据报文 IP 报头中的地址是两端对等体的

地址。

4. 判断题：AH 协议验证整个 IP 报文，所以不适宜用在使用 NAT 的网络中。

5. 判断题：IPSec VPN 中两个对等体配置的 ISAKMP 策略优先级必须相同。

6. 判断题：路由器一个接口上可以应用多个加密图。

7. 网络管理员使用哪个命令可以查看到由预共享密钥配置错误导致 ISAKMP SA 无法建立的情况？（　　）

A. show cryto isakmp sa　　B. show cryto ipsec sa

C. debug cryto isakmp　　D. debug cryto ipsec

8. 判断题：ISAKMP 协议使用 UDP 500 端口进行通信，所以 IPSec VPN 是在应用层保护通信数据安全的协议。

9. 以下哪一项不需要在 Easy VPN 客户端上配置？（　　）

A. ISAKMP 策略，如 ISAKMP SA 的加密算法、散列算法等

B. 反向路由

C. 登录用户名和口令的有关信息

D. Easy VPN 服务器 IP

10. 使用哪条命令可以在 Easy VPN 客户端与服务器建立安全隧道时，将反向路由注入路由表中？（　　）

A. reverse-route　　B. ip route reverse

C. route-reverse　　D. router reverse enable

5.7 实训

5.7.1 站到站 VPN 配置

1. 实训组织

实训学时：100 分钟。

学生分组：2 人/组。

2. 实训目的

通过实训，熟练掌握路由器的预共享密钥站到站 VPN 的安全配置基本操作。

3. 实训环境

（1）安装有 Windows 系统和 Cisco VPN 客户端软件的 PC，每组 2 台。

（2）Cisco 2811 路由器（支持 VPN 功能），每组 2 台。

（3）可划分 VLAN 的交换机 1 台。

（4）UTP 交叉电缆，每组 1 条。

（5）UTP 直通电缆，每组 2 条。

（6）Console 电缆，每组 1 条。

注意保持所有路由器、交换机为出厂配置。

4. 实训准备

实训开始前，按照图 5-26 所示网络拓扑连接好网络，按表 5-10 所示配置网络设备、主机的网络连接。按照第 4 章分支机构 B-1 地址转换方案在实训网络中分支机构 B-1 的边界路由器上配置地址转换，并测试网络连通性。

表 5-10　站到站 VPN 配置实训 IP 分配

接　口		IP 地址/网络前缀	网　关
分公司 1 边界路由器 C3845-2-1-1	Fa0/0	200.100.12.254/24	
	S1/0 或 Fa0/1	200.100.15.205/30	
分支机构 B-1 边界路由器 C3845-2-20-1	Fa0/1.10	200.100.11.14/28	
	Fa0/1.15	10.0.0.30/28	
	Fa0/1.20	10.0.2.254/24	
	Fa0/1.30	10.0.3.254/24	
	S1/0 或 Fa0/1	200.100.15.206/30	
PCa		200.100.12.1/24	200.100.12.254

5. 实训内容

预共享密钥站到站 VPN 配置。

6. 实训指导

(1) 检查网络连通性及网络访问控制配置

在配置 VPN 前，必须保证网络基本连通性。使用 ping、show ip route 等命令检查图 5-26 所示网络中，PCa 是否能够 ping 通 PCb，路由器上路由是否正确。

使用 show ip access-list 命令检查路由器上现有访问控制，是否允许 ISAKMP 协议使用 UDP 500 端口进行访问。

(2) 站到站 VPN 配置

分别在分公司 1 和分支机构 B-1 的边界路由器上配置以下内容。

- 创建定义受保护网络的 ACL eacl-vpn。
- 定义 ISAKMP 策略，优先级为 1。
- 定义预共享密钥为 123。
- 定义变换集 ts-vpn。
- 定义保护流量的 ACL eacl-vpn。
- 定义加密图 map-vpn。
- 将所定义的加密图应用到正确接口上。

分公司 1 边界路由器上具体配置操作如下。

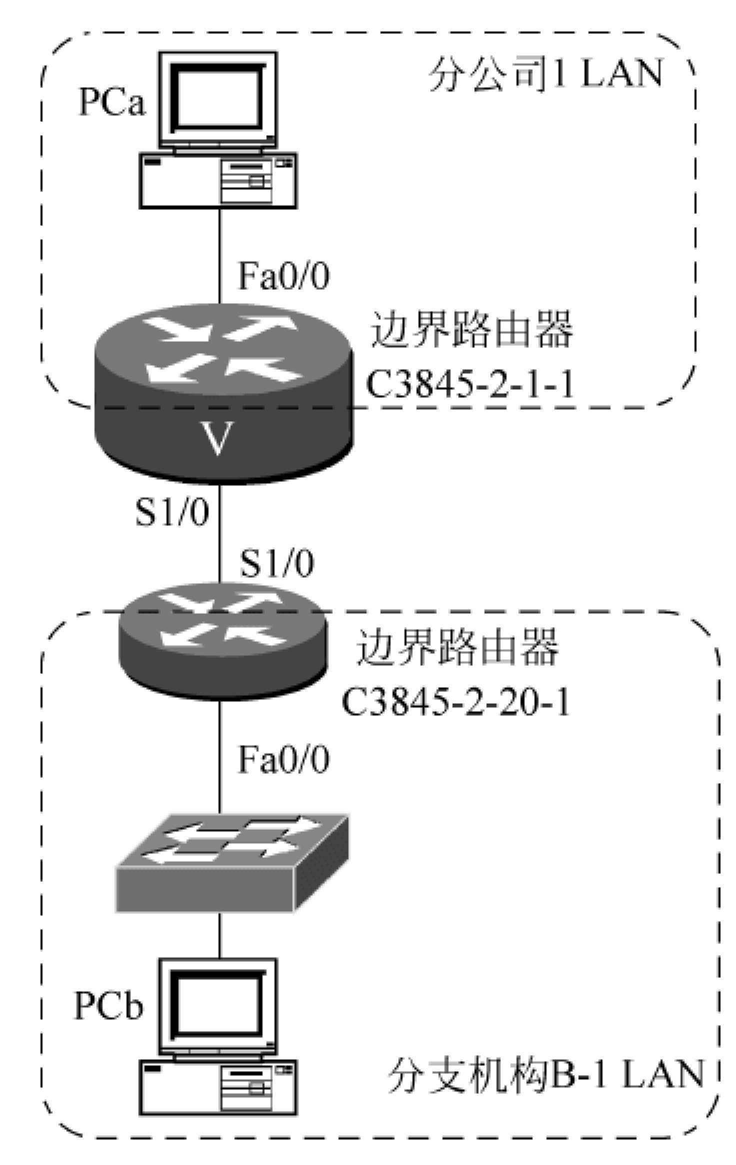


图 5-26　站到站 VPN 配置实训网络拓扑

```
C3845-2-20-1(config)#crypto isakmp policy 1
C3845-2-20-1(config-isakmp)#authentication pre-share
C3845-2-20-1(config-isakmp)#group 2
C3845-2-20-1(config-isakmp)#exit
C3845-2-20-1(config)#crypto isakmp key 123 address 200.100.15.206
C3845-2-20-1(config)#crypto ipsec transform-set ts-vpn esp-md5-hmac esp-3des
C3845-2-20-1(cfg-crypto-trans)#exit
C3845-2-20-1(config)#ip access-list extended eacl-vpn
C3845-2-20-1(config-ext-nacl)#permit ip 200.100.12.0 0.0.0.255 200.100.15.0 0.0.0.63
C3845-2-20-1(config-ext-nacl)#exit
C3845-2-20-1(config)#crypto map map-vpn 10 ipsec-isakmp
C3845-2-20-1(config-crypto-map)#set peer 200.100.15.206
C3845-2-20-1(config-crypto-map)#set transform-set ts-vpn
C3845-2-20-1(config-crypto-map)#match address eacl-vpn
C3845-2-20-1(config-crypto-map)#exit
C3845-2-20-1(config)#interface S1/0
C3845-2-20-1(config-if)#crypto map map-vpn
```

分支机构 B-1 边界路由器上的具体操作如下。

```
C3845-2-20-1(config)#crypto isakmp policy 1
C3845-2-20-1(config-isakmp)#authentication pre-share
C3845-2-20-1(config-isakmp)#group 2
C3845-2-20-1(config-isakmp)#exit
C3845-2-20-1(config)#crypto isakmp key 123 address 200.100.15.205
C3845-2-20-1(config)#crypto ipsec transform-set ts-vpn esp-md5-hmac esp-3des
C3845-2-20-1(cfg-crypto-trans)#exit
C3845-2-20-1(config)#ip access-list extended eacl-vpn
C3845-2-20-1(config-ext-nacl)#permit ip 200.100.15.0 0.0.0.63 200.100.12.0 0.0.0.255
C3845-2-20-1(config-ext-nacl)#exit
C3845-2-20-1(config)#crypto map map-vpn 10 ipsec-isakmp
C3845-2-20-1(config-crypto-map)#set peer 200.100.15.205
C3845-2-20-1(config-crypto-map)#set transform-set ts-vpn
C3845-2-20-1(config-crypto-map)#match address eacl-vpn
C3845-2-20-1(config-crypto-map)#exit
C3845-2-20-1(config)#interface S1/0
C3845-2-20-1(config-if)#crypto map map-vpn
```

(3) 检查 VPN 配置

在配置过程中,使用 show crypto isakmp policy、show crypto ipsec transform-set、show crypto map、debug crypto ipsec、debug crypto isakmp 等命令检查 VPN 配置是否正确。

配置完成后,分别测试 PCb 在不同 VLAN 中能否 ping 通 PCa,分公司 1 边界路由器接口。

7. 实训报告

1. 在进行 VPN 配置前,测试网络连通性。					
PCb	IP 地址/网络前缀	网关	在 PCa 上使用的测试命令	测试结果	解释原因
1	200.100.11.1	200.100.11.14	ping ________	通 □　不通 □	
2	10.0.0.18	10.0.0.30	ping ________	通 □　不通 □	
3	10.0.2.1/24	10.0.2.254	ping ________	通 □　不通 □	
4	10.0.3.1/24	10.0.3.254	ping ________	通 □　不通 □	
2. 在完成 VPN 配置后,测试网络连通性。					
PCb	IP 地址/网络前缀	网关	在 PCa 上使用的测试命令	测试结果	
1	200.100.11.1	200.100.11.14	ping ________	通 □　不通 □	
2	10.0.0.18	10.0.0.30	ping ________	通 □　不通 □	
3	10.0.2.1/24	10.0.2.254	ping ________	通 □　不通 □	
4	10.0.3.1/24	10.0.3.254	ping ________	通 □　不通 □	
3. 当从 PCa 发送 ICMP 数据到分支机构 B-1 边界路由器的接口 S1/0 时,其 IP 报头中:源 IP 地址为:________,目的 IP 地址为:________。					
4. 跟踪 ISAKMP SA、IPSec SA 建立过程,回答问题。(1) VPN 隧道两端对等体上 ISAKMP 策略的优先级是否一定相同?配置不同优先级对 ISAKMP SA 的建立有何影响?(2) 在进行 ISAKMP SA 建立过程中,进行认证的预共享密钥明文是否在网络上传递?(3) 简述 ISAKMP SA 和 IPSec SA 协商建立过程。					

5.7.2 远程访问 VPN 配置

1. 实训组织

实训学时:100 分钟。

学生分组:2 人/组。

2. 实训目的

通过实训,熟练掌握交换机端口安全配置基本操作。

3. 实训环境

(1) 安装有 Windows 系统、网络监听软件(Wireshark)的 PC,每组 2 台。

(2) Cisco 路由器(支持 VPN 功能),每组 1 台。

(3) UTP 直通电缆，每组 2 条。

(4) UTP 交叉电缆，每组 1 条。

(5) Console 电缆，每组 1 条。

注意保持所有的交换机、路由器为出厂配置。

4. 实训准备

实训开始前，按照图 5-27 所示网络拓扑连接好网络，并按表 5-11 所示配置好 PCa、PCb 及路由器各接口 IP 地址、路由等，保证网络连通。

表 5-11 Easy VPN 实训 IP 地址分配

接　　口	IP 地址/网络前缀	网关地址
路由器接口 Fa0/1	200.100.15.206/30	
路由器接口 Fa0/0	10.0.0.1/24	
PCa	200.100.15.205/30	200.100.15.206
PCb	10.0.0.254/24	10.0.0.1

5. 实训内容

远程访问 VPN 配置实现。

6. 实训指导

(1) 配置 Easy VPN Server

在远程访问服务器上，如下配置分支机构 B-1 边界路由器为 Easy VPN Server。

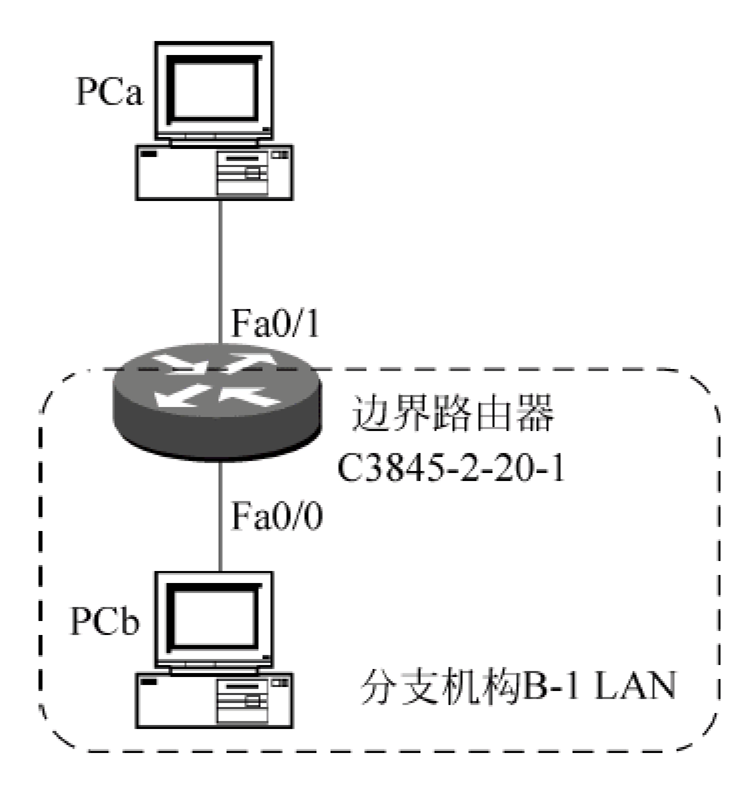


图 5-27 远程访问 VPN 实训网络示意图

```
VPN-Ser(config)#aaa new-model
VPN-Ser(config)# aaa authentication login aaa-rvpn local
VPN-Ser(config)# aaa authorization network aaa-rvpn local
VPN-Ser(config)#username rvpn password 0 123
VPN-Ser(config)#crypto isakmp policy 1
VPN-Ser(config-isakmp)# encrytion 3des
VPN-Ser(config-isakmp)# hash md5
VPN-Ser(config-isakmp)# authentication pre-share
VPN-Ser(config-isakmp)# group 2
VPN-Ser(config-isakmp)# exit
VPN-Ser(config)#ip local pool pool-rvpn 10.0.0.10 10.0.0.20
VPN-Ser(config-isakmp-group)#crypto isakmp client configuration group grp-rvpn
VPN-Ser(config-isakmp-group)# key 123
VPN-Ser(config-isakmp-group)# pool pool-rvpn
VPN-Ser(config-isakmp-group)# include-local-lan
VPN-Ser(config-isakmp-group)# netmask 255.255.255.0
VPN-Ser(config-isakmp-group)# exit
VPN-Ser(config)#crypto ipsec transform-set ts-rvpn esp-3des esp-md5-hmac
VPN-Ser(cfg-crypto-trans)# exit
VPN-Ser(config)#crypto dynamic-map dmap-rvpn 10
VPN-Ser(config-crypto-map)# set transform-set ts-rvpn
```

```
VPN-Ser(config-crypto-map)# reverse-route
VPN-Ser(config-crypto-map)# exit
VPN-Ser(config)#crypto map map-rvpn client authentication list aaa-rvpn
VPN-Ser(config)#crypto map map-rvpn isakmp authorization list aaa-rvpn
VPN-Ser(config)#crypto map map-rvpn client configuration address respond
VPN-Ser(config)#crypto map map-rvpn 10 ipsec-isakmp dynamic dmap-rvpn
VPN-Ser(config)#interface FastEthernet1/0
VPN-Ser(config-if)# crypto map map-rvpn
VPN-Ser(config-if)# exit
VPN-Ser(config)#crypto isakmp keepalive 10
```

(2) 配置 Easy VPN 客户端,建立并测试 VPN 连接

参考 5.3.2 小节配置 PCb 上的 Cisco VPN 客户端,建立 VPN 连接。同时在 Easy VPN 服务器上使用 debug 命令跟踪 ISAKMP SA 和 IPSec SA 建立过程。

在 PCa 上使用 ipconfig 命令检查是否已出现 VPN 客户端建立的虚拟网卡,其 IP 是否为 Easy VPN 服务器端地址池中定义的地址。

在 PCa 上使用 ping 测试能否 ping 通 PCb,并在测试时,使用 Wireshark 软件监听 ESP 报文格式。

7. 实训报告

1. 简述 Easy VPN 服务器配置基本步骤。

2. 如果内部网络地址为 30.0.0.0/24,则 Easy VPN 服务器上的如下命令应修改为什么?
VPN-Ser(config)#ip local pool pool-rvpn ______________________

3. 记录 Wireshark 软件监听到的 ESP 报文结构。

4. VPN 安全隧道建立完成后,在 PCa 上使用 ipconfig 命令查看 PCb VPN 虚拟网络接口的各项配置如下。
以太网适配器 本地连接:
连接特定的 DNS 后缀.........:______________
描述........................:Cisco Systems VPN Adapter
物理地址....................:______________
DHCP 已启用.................:否
自动配置已启用..............:是
IPv4 地址...................:______________
子网掩码....................:______________
默认网关....................:
DNS 服务器..................:10.0.0.1
TCP/IP 上的 NetBIOS.........:已启用

5. VPN 安全隧道建立完成后,在 PCa 上测试到 PCb 的网络连通性的命令及结果如下。
ping ______________。通 □ 不通 □

第 6 章

防　火　墙

本章任务：根据工程任务安全需求分析，解决网络边界安全中防火墙基本配置问题。

必备知识：（1）防火墙工作原理。

（2）防火墙网络连通性配置。

（3）防火墙 VPN 配置。

学习目标：完成模拟公司网络边界防火墙的安全配置，防御来自 Internet 的安全威胁。

6.1　模拟公司总部网络内外网边界安全任务分析

模拟公司总部网络安全通信需求如下。

（1）模拟公司总部 Web 服务器、邮件服务器需对外提供 24 小时服务。

（2）模拟公司总部网络内主机可以访问 Internet 上各种资源，但非公司所属机构的外部网络主机，不能主动连接模拟公司总部网络内主机。

（3）模拟公司总部与分支机构网络间所有通信，需进行加密保护。

（4）网管员需能利用 Internet 线路，在受保护的安全通道上远程管理总部的网络设备。

以上安全通信需求虽然可以使用配置了 ACL 的路由器来实现，但路由器的主要功能是进行数据转发和路由，当网络流量较大时，难以保障网络性能。为解决网络安全与性能间的矛盾，模拟公司总部网络选择在网络边界上配置硬件防火墙来完成网络通信过滤等安全功能，如图 6-1 所示。

但要满足以上所述通信安全需求，在防火墙上还需完成以下配置。

（1）基本网络连通性配置。

（2）配置访问控制，允许外部网络访问内部 Web、邮件服务。

（3）配置访问控制，允许外部网络对内部网络已建立连接的访问，但禁止所有其他 TCP 连接。

（4）配置 VPN，保障模拟公司总部与分支机构网络间通信。

（5）配置 VPN，保障网管员能远程访问模拟公司总部网络内的网络设备。

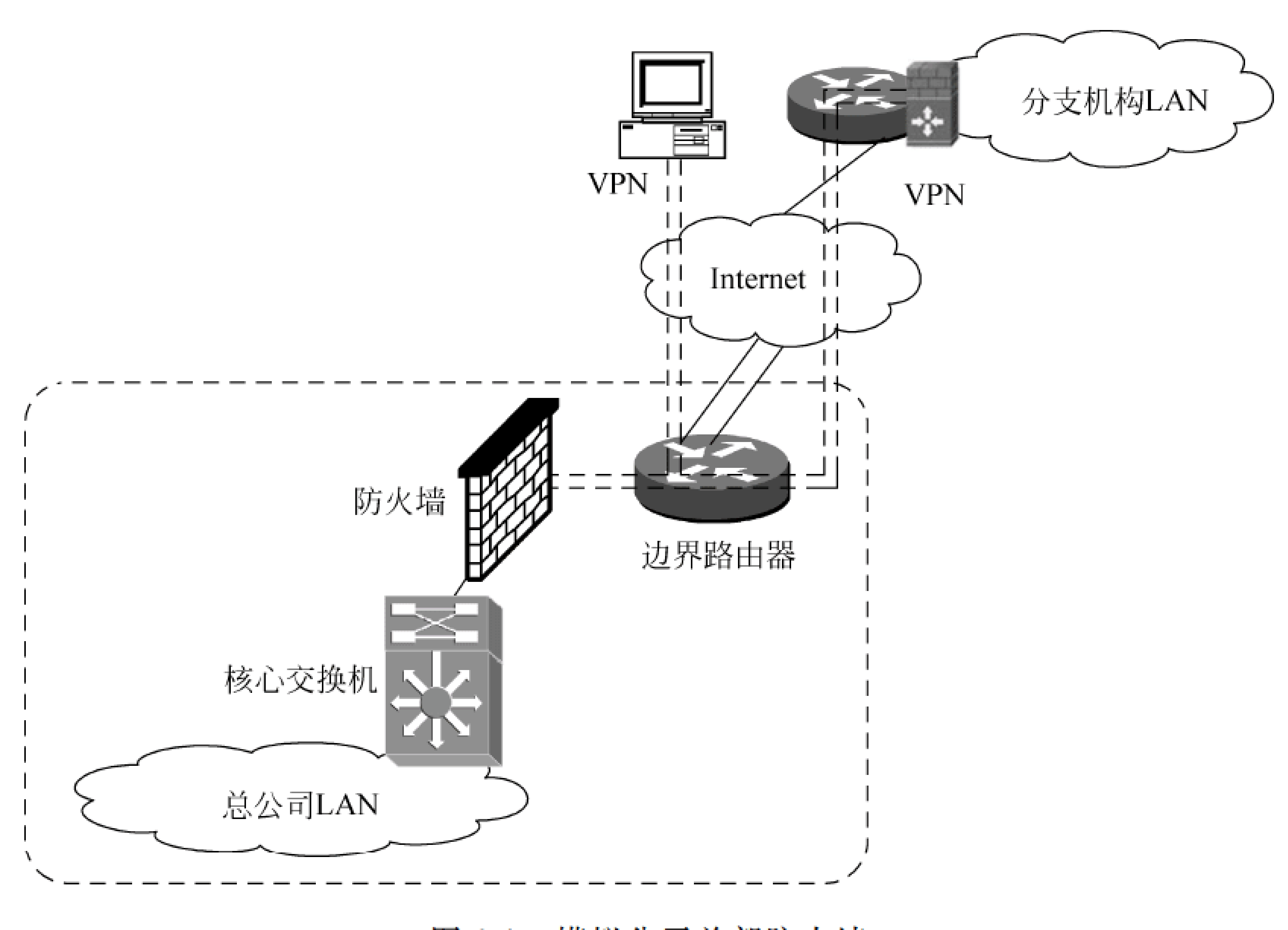


图 6-1　模拟公司总部防火墙

6.2　防火墙简介

1. 防火墙概念及类型

防火墙(Firewall)一词在计算机网络中用来代表在网络间进行访问控制的系统。它可以是软件,如运行在用户计算机上防御恶意攻击或非法访问的个人防火墙软件;也可以是硬件,与使用 ACL 的路由器相比,硬件防火墙使用专用硬件、软件对网络间访问进行控制,可以在不影响网络性能的情况下提供安全保障。

按工作方式分,防火墙有“包过滤”、“代理服务器”和“基于状态的包过滤”3 种。

(1)“包过滤”类似于无状态 ACL,防火墙根据报头信息对进入网络的报文进行过滤,不会记录内外通信会话状态信息。

(2)“代理服务器”防火墙会代替内部网络主机向外部网络服务器发出请求,并将响应反馈给内部网络主机,然而缓存请求与响应都需要消耗大量系统资源。

(3)“基于状态的包过滤”防火墙类似于 CBAC,通过记录会话状态信息对进入网络的报文进行过滤。

2. 防火墙默认访问控制规则

防火墙产品在访问控制方面一般都有一些默认处理规则,例如 Cisco 防火墙产品 PIX 使用 ASA(Adapter Security Appliances,适应性安全算法)对通过防火墙的流量进行过滤,ASA 默认的报文过滤规则如下。

(1) 在没有任何有关状态信息情况下,Cisco PIX 防火墙不允许任何报文穿过防火墙。

(2) 从 Cisco PIX 防火墙接口进入的报文不能再从同一接口流出。

(3) 出站(outbound)连接默认是被允许的,除非配置了禁止的 ACL 条目。注意,出站报文是指从防火墙高安全级别接口流向低安全级别接口的报文。

(4) 入站(inbound)连接默认是被禁止的,除非配置了允许的 ACL 条目。注意,入站报文是指从防火墙低安全级别接口流向高安全级别接口的报文。

(5) 如果不进行特别配置,则 ICMP 报文均被禁止。

(6) 防火墙在按上述规则过滤报文时,会记录系统日志。

3. 接口安全级别与 DMZ

Cisco PIX 防火墙防火墙使用 0～100 的数字来定义安全级别,接口安全级别数字越大,表示接口安全级别越高,接口所连接的网络越应受到更高安全保护。

Cisco PIX 防火墙支持为接口命名,以便于管理。inside、outside 和 dmz 为防火墙上 3 个带有特定含义的接口名。

inside 接口默认安全级别为 100,安全级别最高,一般用于连接内部网络。

outside 接口默认安全级别为 0,安全级别最低,一般用于连接外部网络。

dmz 接口默认安全级别为 0,安全级别也最低,用于连接非军事化区网络(demilitarized zone)。非军事化区网络是企业内部网络中在安全级别比外部网络高,但比内部网络低的网络,企业内部网络中那些需要对外提供网络服务的服务器被放置在非军事化区网络中,这样有利于保护企业内部网络中的其他主机。

6.3 网络连通性配置

任何网络设备加入到网络中时,配置网络连通性都是第一项要做的工作,Cisco PIX 防火墙也不例外。与路由器的网络连通性配置类似,Cisco PIX 防火墙网络连通性配置的基本步骤如表 6-1 所示。

表 6-1 Cisco PIX 防火墙网络连通性配置步骤

序 号	操 作	相 关 命 令	是否必要
步骤 1	配置接口名	**nameif**	是
步骤 2	配置接口优先级	**security-level**	根据情况使用
步骤 3	配置接口地址	**ip address**	是
步骤 4	启用接口	**no shut**	是
步骤 5	配置路由	**route**、**router** 等	是
步骤 6	配置地址转换	**global**、**nat** 或 **static**	非透明模式必要
步骤 7	配置访问控制	**access-list** **access-group**	是
步骤 8	检查网络连通性	**show interface ip**、**show ip address**、**show route**、**ping** 等	可选

6.3.1 接口及路由配置

1. 配置接口名

Cisco PIX 防火墙接口只有被命名后,其 IP 功能才能启用。在 Cisco PIX 防火墙上,

为接口命名的操作是在接口配置模式下输入：

nameif　接口名

参数“接口名”用于定义该防火墙接口的名字，该名字为一个小于 49 个字符长度的字符串。如果使用 inside 命名接口，则接口优先级自动被设置为 100，而设置为 outside、dmz 或其他字符串时，接口优先级均被自动设置为 0。

2. 配置接口安全级别

如上所述，Cisco PIX 防火墙在配置接口名时，系统会自动为其分配安全级别。但如果自动分配的安全级别与所需不符，则可以在接口配置模式下输入：

security-level　安全级别

参数“安全级别”用于定义所需的安全级别数值，范围为 0～100。

3. 检查接口 IP 地址配置

在 Cisco PIX 防火墙上，检查接口 IP 地址配置情况的操作命令与路由器上稍有不同。

在特权模式下输入：

show　interface　ip　brief　①

或者

show　ip　address　[outside | inside]　②

都可以查看接口上 IP 地址配置情况，但使用命令①还可以查看到接口当前链路状态，而命令②可以查看到接口名配置情况。

在 Cisco PIX 防火墙上，分别使用命令①、②查看接口 IP 地址配置情况的输出结果如下。

```
fw# show ip address
System IP Addresses:
Interface          Name        IP address      Subnet mask       Method
Ethernet0          outside     10.0.0.254      255.255.255.0     manual
Ethernet4          inside      10.1.1.1        255.255.255.0     manual
Current IP Addresses:
Interface          Name        IP address      Subnet mask       Method
Ethernet0          outside     10.0.0.254      255.255.255.0     manual
Ethernet4          inside      10.1.1.1        255.255.255.0     manual
fw# show interface ip brief
Interface              IP-Address      OK           Method Status
Protocol
Ethernet0              10.0.0.254      YES          manual up
up
Ethernet1              unassigned      YES unset    administratively down up
Ethernet2              unassigned      YES unset    administratively down up
Ethernet3              unassigned      YES unset    administratively down up
Ethernet4              10.1.1.1        YES          manual up
up
```

6.3.2 路由配置及检查

由于防火墙的主要功能不是进行路由，所以 Cisco PIX 防火墙支持的动态路由协议有限，可以支持 RIP、OSPF 等，在 Cisco PIX 防火墙上配置动态路由的命令与 Cisco IOS 路由器上相同。

在 Cisco PIX 防火墙上配置静态路由的操作为在全局模式下输入：

route 接口名 目的网络地址 子网掩码 网关 IP [度量值]

参数"目的网络地址"、"子网掩码"用于定义路由中的目的网络。

参数"网关 IP"用于定义防火墙到达目的网络的网关（下一跳）地址。

参数"度量值"定义该路由到达目的网络的距离。

参数"接口名"定义要到达目的网络防火墙的送出接口。

在 Cisco PIX 防火墙上配置 OSPF 动态路由协议的基本操作与路由器相似，在全局模式下输入如下命令，可以完成启用 OSPF 路由进程，并配置路由发布网络的操作。

router ospf OSPF 进程号
  network 网络号 子网掩码 **area** 区域号

注意：在防火墙上发布网络时，使用"子网掩码"而不是通配符。

配置完路由后，可以在 Cisco PIX 防火墙上使用 show 命令查看防火墙路由表，以检查路由配置。具体操作为在特权模式下输入：

show route

该命令输出结果如下。

```
fw# show route

Codes: C-connected, S-static, I-IGRP, R-RIP, M-mobile, B-BGP
       D-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF inter area
       N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2
       E1-OSPF external type 1, E2-OSPF external type 2, E-EGP
       i-IS-IS, L1-IS-IS level-1, L2-IS-IS level-2, ia-IS-IS inter area
       *-candidate default, U-per-user static route, o-ODR
       P-periodic downloaded static route

Gateway of last resort is not set

C      10.1.1.0 255.255.255.0 is directly connected, inside
C      10.0.0.0 255.255.255.0 is directly connected, outside
S      200.100.10.0 255.255.255.0[1/0]via 10.0.0.1, outside
```

6.3.3 地址转换配置

根据 Cisco PIX 防火墙默认访问控制规则，必须配置相应的访问控制，允许必要的外网流量进入防火墙，才能实现内外网通信。但对于工作在非透明模式的防火墙，只有配置地址转换后，访问控制列表才能够发挥功效。因此为实现网络连通性，还需先配置内外网

地址转换。

另外，防火墙作为独立的安全设备，相对路由器能够保存更多的地址转换信息，因此比路由器更适于完成网络的地址转换功能。

1. 静态 NAT 配置

在 Cisco PIX 防火墙上配置静态 NAT 的操作步骤如表 6-2 所示。与在路由器上配置 NAT 相比，在 Cisco PIX 防火墙上配置址转换映射条目时，将地址转换应用的接口及地址映射一并定义，所以省略了定义地址转换内、外网接口的步骤。

表 6-2 静态 NAT 配置步骤

序 号	操 作	相 关 命 令	是否必要
步骤 1	定义地址转换映射条目	**static**	是
步骤 2	检查地址映射配置	**show xlate** **show conn**	可选

(1) 定义地址转换映射条目

在 Cisco PIX 防火墙上，配置静态 NAT 地址转换映射条目的操作为在全局配置模式下输入：

static (接口名 a，接口名 b) 全局地址或映射地址 { 原 IP 地址 [**netmask** 子网掩码]|
access-list ACL 名 }

参数对“(接口名 a，接口名 b)”用于定义地址转换在哪两个接口间进行。排在左边的接口名为地址转换的原接口或内部接口，排在右边的为地址转换的映射接口或外部接口。

参数“全局地址或映射地址”用于指定地址被转换为哪个全局地址或映射地址。

参数“原 IP 地址”用于指定被转换的地址。可以使用关键字 network 及参数“子网掩码”配合参数“原 IP 地址”定义一个原地址段以进行一个网络到另一个网络的静态一对一地址转换。该命令中也可以使用关键字 access-list 及参数“ACL 名”来代替参数“原地址”，定义要被转换的地址段。

例如，如果要将内部网络 10.0.0.0/24 的地址转换为公共 IP 地址段 200.100.10.0/24，则相应的命令如下。

```
fw(config)# static (inside,outside) 200.100.10.0 10.0.0.0 netmask 255.255.255.0
```

又如，如果要将外部重叠网络的地址 200.100.10.1 转换为 10.1.10.1，则相应命令如下。

```
fw(config)# static (outside,inside) 10.1.10.1 200.100.10.1
```

(2) 检查地址映射配置

在 Cisco PIX 防火墙的特权模式下输入 show xlate 命令，可以检查地址转换映射条目配置，其输出结果如下。

```
fw# show xlate
1 in use, 1 most used
```

```
Global   200.100.10.0   Local   10.0.0.0
```

在特权模式下输入 show conn 命令，可以查看当前防火墙上通信会话情况，其输出结果如下，配合 show xlate 命令可以查看当前内网哪些主机正在通过地址转换与外网主机通信。

```
fw# show conn
16 in use, 22 most used
ICMP out 200.200.200.200:0 in 10.0.0.253:3637 idle 0:00:01 bytes 72
ICMP out 200.200.200.200:0 in 10.0.0.253:3636 idle 0:00:01 bytes 72
```

该输出结果显示内部主机 10.0.0.253 与外部主机 200.200.200.200 之间在进行 ICMP 会话。

2. 动态 NAT 配置

在 Cisco PIX 防火墙上定义动态 NAT 的配置步骤如表 6-3 所示。

表 6-3 动态 NAT 配置步骤

序 号	操 作	相 关 命 令	是否必要
步骤 1	定义转换后地址池	**global**	是
步骤 2	定义被转换地址范围	**nat**	是
步骤 3	检查 NAT 转换配置	**show xlate**	可选

当在 Cisco PIX 防火墙上配置动态 NAT 时，需分别使用 global 和 nat 命令定义地址池和被转换的地址范围。

(1) 定义转换后地址池

在 Cisco PIX 防火墙上，定义地址池的操作为在全局配置模式下输入：

global (接口名)地址转换条目序号 { 地址 | 起始地址-结束地址 }

参数“接口名”指定全局地址对应的接口。例如对于内部地址转换，此处应为连接外部网络的接口的名字；而对于外部地址转换，此处应为连接内部网络的接口的名字。

参数“地址转换条目序号”是从 0～2147483647 的序号，该序号用于将 global 命令定义的地址池和 nat 命令定义的需被转换地址绑定在一起。

参数“地址”或参数“起始地址-结束地址”用于定义全局地址池范围。

(2) 定义被转换地址范围

在 Cisco PIX 防火墙上，定义被转换地址范围的操作为在全局配置模式下输入：

nat (接口名)地址转换条目序号 { 地址[**netmask** 子网掩码]} | **access-list** ACL 名 }

参数“接口名”指定被转换地址来自哪个接口。例如对于内部地址转换，此处应为连接内部网络的接口的名字。

参数“地址转换条目名”与 global 命令中的地址转换条目名参数相对应。

参数“地址”与关键字 netmask、参数“子网掩码”用于定义被转换地址的范围，如果此处“地址”为 0，则表示所有地址。关键字 access-list 和参数“ACL 名”可以替换参数“地

址”等用于定义被转换地址的范围。

例如，若要进行内部地址转换，将内部网络 10.0.0.0/24 中所有地址动态转换到 200.100.10.0/24，则可以如下定义。

```
fw(config)# global (outside) 1 200.100.10.8-200.100.10.17
fw(config)# nat (inside) 1 10.0.0.0 255.255.255.0
```

(3) 检查动态 NAT 配置

在配置动态 NAT 后，由于是动态从地址池选择地址进行转换，因此在没有内外通信连接时，使用 show xlate 命令看不到任何转换条目，如下所示。

```
fw# show xlate
0 in use, 1 most used
```

当内外网有通信连接时，使用 show xlate 命令会看到动态形成的地址转换映射，如下所示。

```
fw# show  xlate
0 in use, 1 most used
fw# show xlate
1 in use, 1 most used
Global 200.100.10.8 Local 10.0.0.253
```

(4) 配置防火墙不进行地址转换

注意：当 nat 命令中地址转换条目序号为 0，防火墙不进行地址转换。

例如，若不需防火墙实现地址转换，但为保证内外网络能通过防火墙进行通信，可以配置一条序号为 0 的 nat 实现，如下所示。

```
fw(config)# nat (inside) 0 10.0.0.0 255.255.255.0
```

此时使用 show xlate 命令查看地址转换映射，会发现内部地址未被转换，而是直接使用内部地址。

```
fw# show  xlate
1 in use, 1 most used
Global  10.0.0.253  Local  10.0.0.253
```

3. 动态 PAT 配置

在 Cisco PIX 防火墙上定义动态 PAT 的操作与配置动态 NAT 相似，只是使用 global 命令定义地址池时语法稍有不同。

(1) 定义重载到接口的 PAT 转换

在 Cisco PIX 防火墙上，定义重载到某个接口的动态 PAT 转换操作为在全局配置模式下输入：

global (接口名)地址转换条目序号 **interface**

使用该命令可以将地址重载到参数“接口名”指定的接口地址上。

例如，将内部网络所有地址重载到外部接口 outside 的配置操作过程，以及使用 show xlate 命令显示地址转换条目输出的结果如下。

```
fw(config)# nat (inside) 1 0
fw(config)# global (outside) 1 interface
INFO: outside interface address added to PAT pool
fw(config)# exit
fw# show xlate
1 in use, 1 most used
PAT Global 200.100.10.254(1024) Local 10.0.0.253(11002)
```

(2) 定义重载到某个地址的 PAT 转换

在 Cisco PIX 防火墙上，定义重载到某个地址的动态 PAT 转换操作为在全局配置模式下输入：

global (接口名)地址转换条目序号 地址

注意：在 Cisco PIX 防火墙上一条 global 命令只能重载到一个 IP 地址，所以要定义重载到多个公共 IP 地址，需要使用多条地址转换条目序号相同的 global 命令。

例如，将内网所有地址重载到公共 IP 地址 200.100.10.8、200.100.10.9 的配置过程如下。

```
fw(config)# nat (inside) 1 0
fw(config)# global (outside) 1 200.100.10.8
INFO: Global 200.100.10.8 will be Port Address Translated
fw(config)# global (outside) 1 200.100.10.9
INFO: Global 200.100.10.9 will be Port Address Translated
fw(config)# exit
fw# show xlate
11 in use, 11 most used
Global 10.0.0.253 Local 10.0.0.253
PAT Global 200.100.10.8(10)Local 10.1.1.1 ICMP id 6594
PAT Global 200.100.10.8(9)Local 10.1.1.1 ICMP id 6593
PAT Global 200.100.10.8(8)Local 10.1.1.1 ICMP id 6592
PAT Global 200.100.10.8(7)Local 10.1.1.1 ICMP id 6591
PAT Global 200.100.10.8(6)Local 10.1.1.1 ICMP id 6590
PAT Global 200.100.10.8(15)Local 10.2.2.1 ICMP id 8676
PAT Global 200.100.10.8(14)Local 10.2.2.1 ICMP id 8675
PAT Global 200.100.10.8(13)Local 10.2.2.1 ICMP id 8674
PAT Global 200.100.10.8(12)Local 10.2.2.1 ICMP id 8673
PAT Global 200.100.10.8(11)Local 10.2.2.1 ICMP id 8672
```

注意：在 Cisco PIX 防火墙上可以同时将一段地址映射到 NAT 和 PAT。当地址池 200.100.10.8～200.100.10.17 的地址被用尽时，可以使用 200.100.10.18 的 PAT 来补充外部地址。

```
fw(config)# nat (inside) 1 0
fw(config)# global (outside) 1 200.100.10.8-200.100.10.17 netmask 255.255.255.0
INFO: Global 200.100.10.8 will be Port Address Translated
```

fw(config)# **global (outside) 1 200.100.10.18 netmask 255.255.255.0**
INFO: Global 200.100.10.9 will be Port Address Translated

4. 端口重定向配置

在 Cisco PIX 防火墙上,配置端口重定向地址转换的操作为在全局配置模式下输入:

static (接口名 a,接口名 b) { **tcp** | **udp** }{全局地址或映射地址 | **interface**} 全局端口或映射端口 { 原 IP 地址[**netmask** 子网掩码]| **access-list** ACL 名 } 原端口或被转换的端口

例如,将内部 Web 服务器 10.0.0.253:8080 映射为 200.100.10.8:80 的配置过程及检查操作如下。

fw(config)# **static (inside,outside) tcp 200.100.10.8 www 10.0.0.253 8080**
fw# **show xlate**
2 in use, 11 most used
PAT Global 200.100.10.8(80)Local 10.0.0.253(8080)

6.3.4 无状态访问控制配置

在 Cisco PIX 防火墙上配置访问控制列表的操作与在路由器非常相像,如表 6-4 所示,但实际上语法和配置模式还是有所不同。

表 6-4 Cisco PIX 防火墙无状态 ACL 配置步骤

序 号	操 作	相关命令	是否必要
步骤 1	定义 ACL	**access-list**	是
		icmp permit|**deny**	根据工程实际需要配置
步骤 2	应用 ACL	**access-group**	是
步骤 3	检查 ACL 配置	**show access-list**	可选

1. 定义 ACL

Cisco PIX 防火墙使用 access-list 命令定义命名 ACL。

在 Cisco PIX 防火墙上,配置无状态标准 ACL 的操作为在全局配置模式下输入:

access-list ACL 名 **standard** { **permit** | **deny** } {目的主机名 | 目的网络地址 子网掩码 | **any** | **host** 目的主机地址 }

在 Cisco PIX 防火墙上,配置无状态扩展 ACL 的操作为在全局配置模式下输入:

access-list ACL 名 [**line** 条目序号] **extended** { **permit** | **deny** } 协议号或协议名 {目的主机名 | 目的网络地址 子网掩码 | **any** | **host** 目的主机地址 }{源主机名 | 源网络地址 子网掩码 | **any** | **host** 源主机地址 }

对于 TCP、UDP 协议,配置无状态扩展 ACL 时,其命令语法为:

access-list ACL 名 [**line** 条目序号]**extended** { **permit** | **deny** } **tcp**|**udp** {目的主机名 | 目的网络地址 子网掩码 | **any** | **host** 目的主机地址 | **interface** 接口名 }{运算符 端口 }{源主机名 | 源网络地址 子网掩码 | **any** | **host** 源主机地址 | **interface** 接口名 }{运算符 端口 }

access-list 命令使用的大部分参数含义与路由器上无状态 ACL 定义中的参数相同,

可参考第 2 章有关内容。

Cisco PIX 防火墙对 ACL 的处理规则与路由器相同，ACL 条目的顺序非常重要，因此如果需要在已有 ACL 中插入访问控制条目，可以使用关键字 line 和参数“条目序号”指定访问控制条目的插入位置。注意，只有扩展 ACL 才支持该功能。

2. 应用 ACL

在 Cisco PIX 防火墙的全局配置模式下配置应用 ACL。应用 ACL 的命令语法如下。

access-group ACL 名 ｛ **in** | **out** ｝ **interface** 接口名

注意：防火墙默认禁止从低安全级别接口到高安全级别接口的流量，所以为保证内外网能够通信，必须配置允许从低安全级别接口到高安全级别接口的返回流量。另外，Cisco PIX 防火墙默认不允许任何 ICMP 报文通过，所以要使用 ping 测试网络连通性，必须进行相应配置允许合法的 ICMP 报文能够通过防火墙。

3. 防火墙对 ICMP 流量的访问控制

防火墙默认不允许低安全级别接口 ICMP 流量入站访问高安全级别接口，所以如图 6-2 所示，如果 e0 接口为低安全级别接口，e1 接口为高安全级别接口，则只有正确配置了地址转换和允许 e0 的入站 ICMP 流量后，网络 1 才能 ping 通网络 2。

另外，Cisco PIX 防火墙被设计为永远禁止“远端接口”的 ICMP 流量，但默认允许“近端接口”的 ICMP 流量。如图 6-2 所示，防火墙 e1、e0 接口分别为网络 1、2 近端接口，所以网络 1 主机能够 ping 通接口 e1，网络 2 主机能够 ping 通接口 e0。但网络 1 主机永远不能 ping 通防火墙 e0 接口，网络 2 主机也不能 ping 通防火墙 e1 接口。

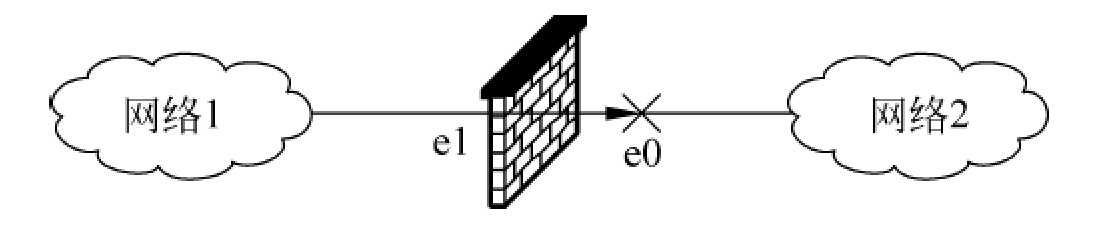


图 6-2　防火墙接口 ICMP 访问示意图

如果希望防火墙近端接口也不响应 ICMP 流量，即让网络上主机无法通过 ping 发现防火墙，则可以使用 ICMP 命令禁止对近端接口的 ICMP 访问。在全局配置模式下输入：

icmp deny ｛ 主机名 | 网络地址 子网掩码 | **any** | **host** 主机地址 ｝[ICMP 报文类型或序号]接口名

例如，可以输入如下命令禁止图 6-2 中防火墙接口 e1 发出或响应 ICMP 报文。

fw(config)# **icmp deny any outside**

6.4 VPN 配置

如前所述，由于实现 VPN 技术需要对等体网络设备进行大量加密、验证运算处理，而这些处理又非常消耗系统资源，所以从保证网络性能角度出发，防火墙或硬件 VPN 设备都比路由器更适于承担 VPN 对等体的角色。

6.4.1　站到站 VPN 配置

在 Cisco PIX 防火墙上，配置站到站 IPSec VPN 的步骤如表 6-5 所示，其步骤与 Cisco IOS 路由器基本相同，只是命令语法稍有不同。

表 6-5　在 Cisco PIX 防火墙上进行站到站 IPSec VPN 配置的步骤

序　号	操　　作	相 关 命 令	必　　要
步骤 1	定义 ISAKMP 策略	**[crypto]isakmp policy**	是
步骤 2	定义 ISAKMP 预共享密钥	**[crypto]isakmp key**	使用预共享密钥时必要
步骤 3	在接口上启用 ISAKMP	**isakmp enable outside**	是
步骤 4	定义变换集	**[crypto]ipsec transform-set**	是
步骤 5	定义保护的流量	**access-list**	是
步骤 6	创建加密图	**crypto map**	是
步骤 7	应用加密图	**crypto map...interface**	是
步骤 8	检查 VPN 配置	**show crypto isakmp sa** **show crypto ipsec sa**	可选

(1) 定义 ISAKMP 策略

在 Cisco PIX 防火墙 8.2 版本系统中，定义 ISAKMP 策略的操作与在路由器的配置基本相同，仅个别参数不同。在全局配置模式下，输入以下命令会进入 ISAKMP 策略配置模式。

[crypto]　**isakmp**　**policy**　ISAKMP 策略优先级

在防火墙上，crypto 可省，可以直接输入 isakmp policy 定义 ISAKMP 策略。参数“ISAKMP 策略优先级”与路由器中含义相同，取值范围是 1～65535。

进入 ISAKMP 策略配置模式后，同样可以输入以下子命令分别定义 D-H 组、认证模式、加密算法、散列算法、ISAKMP SA 生存时间。

group 1 | **2** | **5** | **7**
authentication pre-share | **rsa-sig**
encryption { **3des** | **aes** | **aes-192** | **aes-256** | **des** }
hash { **md5** | **sha** }
lifetime ISAKMP SA 生存时间

注意： 如果参数“ISAKMP SA 生存时间”配置为 none，则表示不对生存时间进行限制。在 Cisco PIX 525 防火墙上，该生存时间范围是 120～2147483647 秒。

(2) 在外部端口上启用 ISAKMP

在 Cisco PIX 防火墙 8.2 版本系统中，需要指定在哪个端口允许 ISAKMP 协议流量通过，具体配置操作为在全局配置模式下输入：

isakmp enable　接口名

一般由外部接口 outside 监听 ISAKMP 流量，所以可以进行如下操作。

```
fw(config)# isakmp enable outside
```

(3) 定义 ISAKMP 预共享密钥

在 Cisco PIX 防火墙上,定义对等体认证预共享密钥的操作与在 Cisco IOS 路由器上的操作相同,即在全局配置模式下输入:

crypto isakmp key 预共享密钥[**address** 远端对等体 IP 地址 远端对等体子网掩码 | **hostname** 远端对等体主机名]

(4) 定义变换集

在 Cisco PIX 防火墙上,定义变换集的操作为在全局配置模式下输入:

crypto ipsec transform-set 变换集名 加密或认证算法[...]

而定义 VPN 以传输模式工作的操作是在全局配置模式下输入:

crypto ipsec transform-set 变换集名 **mode transport**

(5) 定义保护的流量

在 Cisco PIX 防火墙上使用 ACL 定义 VPN 保护的流量时,与路由器上相似。

- VPN 保护 ACL 中 permit 允许的流量。
- 防火墙会丢弃本应受 VPN 保护却没有被保护处理的入站流量。
- 防火墙只接受 ACL 中 permit 允许流量的 IPSec SA 请求。

例如,要在总部网络 200.100.8.0/22 与分支机构 A-1 网络 200.100.12.0/24 间建立 VPN 连接,则 ACL 可如下定义。

```
fw0(config)#access-list eacl-c2a1vpn permit ip 200.100.8.0 255.255.252.0  200.100.12.0  255.255.255.0
```

(6) 创建加密图

在 Cisco PIX 防火墙上,需要使用多条命令分别配置加密图中的远端对等体地址、受保护的流量、变换集等,其操作为在全局配置模式下输入:

crypto map 加密图名 加密图条目序号 **match address** ACL 名或序号
crypto map 加密图名 加密图条目序号 **set peer** 远端对等体的主机名或 IP 地址
crypto map 加密图名 加密图条目序号 **set transform-set** 变换集名

(7) 应用加密图

在 Cisco PIX 防火墙上,应用加密图不需要进入接口配置模式,而是在全局配置模式下输入:

crypto map 加密图名 **interface** 接口名

例如,在接口 outside 上应用加密图 map-c2a1vpn 的操作如下。

```
fw(config)# crypto map map-c2a1vpn interface outside
```

6.4.2 远程访问 VPN 配置

在 Cisco PIX 防火墙上配置远程访问 VPN 的操作步骤如表 6-6 所示,与站到站 VPN

配置相比，主要有两处不同：增加了组策略和动态加密图的定义；在组策略中定义对等体间认证所需预共享密钥。

表 6-6　Cisco PIX 远程访问 VPN 配置步骤

序　号	操　　作	相关命令	必要
步骤 1	定义 ISAKMP 策略	[crypto]isakmp policy	是
步骤 2	在接口上启用 ISAKMP	isakmp enable outside	是
步骤 3	配置组策略参数	tunnel-group	是
步骤 4	定义变换集	[crypto]ipsec transform-set	是
步骤 5	创建动态加密图	crypto dynamic-map	是
步骤 6	创建静态加密图，并将动态加密图加入到静态加密图中	crypto map	是
步骤 7	应用加密图	crypto map... interface	是
步骤 8	检查 VPN 配置	show crypto isakmp sa show crypto ipsec sa	可选

以上步骤中，与站到站 VPN 配置相同的部分不再赘述，参考前面有关内容。

（1）配置组策略参数

在 Cisco PIX 防火墙上配置组策略时，需要定义 3 个基本参数：组策略对应的 VPN 类型、预共享密钥、本地地址池。

定义组策略 VPN 类型的操作应在进行组策略其他配置前进行。在全局配置模式下，输入如下命令将创建一个指定类型的组策略。

tunnel-group 组策略名 **type** VPN 类型

当为远程访问 VPN 定义组策略时，参数“VPN 类型”为 remote-access；如果为站到站 VPN 定义组策略，则需使用 ipsec-l2l。

对于使用预共享密钥方式的远程访问 VPN，应在其组策略中定义预共享密钥。在全局配置模式下输入如下命令进入“组策略-IPSec 属性”配置模式，使用 pre-shared-key 子命令将为该组定义一个预共享密钥。

tunnel-group 组策略名 **ipsec-attributes**
　pre-shared-key 预共享密钥

定义远程访问 VPN 使用哪个本地地址池的操作为，在全局配置模式下输入如下命令进入“组策略-一般属性”配置模式，然后使用 address-pool 子命令，可以为该组定义使用的地址池。

tunnel-group 组策略名 **general-attributes**
　address-pool 地址池名

（2）创建动态加密图

在 Cisco PIX 防火墙上也需创建动态加密图，并在动态加密图中配置变换集和反向路由。其配置操作为在全局配置模式下输入：

crypto dynamic-map 动态加密图名 动态加密图条目号 **set transform-set** 变换集名

crypto dynamic-map 动态加密图名 动态加密图条目号 **set reverse-route**

（3）创建静态加密图并将动态加密图加入到静态加密图中

在 Cisco PIX 防火墙上，创建静态加密图并将动态加密图加入到静态加密图中，操作为在全局配置模式下输入：

crypto map 加密图名 加密图条目号 **ipsec-isakmp dynamic** 动态加密图名

（4）应用加密图

在 Cisco PIX 防火墙上，应用加密图的操作为在全局配置模式下输入：

crypto map 加密图名 **interface** 接口名

例如，为一个防火墙配置远程访问 VPN。该防火墙内网地址为 10.0.0.0/24，定义本地地址池 10.0.0.200～10.0.0.250，创建登录用户 rvpn，口令为 123 等。其配置如下。

```
!ISAKMP 策略
isakmp policy 1
authentication pre-share
hash sha
group 2
encryption 3des
isakmp enable outside
!地址池
ip local pool pool-rvpn 10.0.0.200-10.0.0.250 mask 255.255.255.0
!本地认证账号
username rvpn password 123
!变换集
crypto ipsec transform-set ts-rvpn esp-3des esp-md5-hmac
!组策略
tunnel-group tg-rvpn type remote-access
tunnel-group tg-rvpn general-attributes
  address-pool pool-rvpn
tunnel-group tg-rvpn ipsec-attributes
  pre-shared-key 123
!动态加密图
crypto dynamic-map dmap-rvpn 1 set transform-set ts-rvpn
crypto dynamic-map dmap-rvpn 1 set reverse-route
!静态加密图
crypto map map-rvpn 10 ipsec-isakmp dynamic dmap-rvpn
!应用静态加密图
crypto map map-rvpn interface outside
```

6.5 模拟公司总部边界防火墙配置方案

根据 6.1 节安全配置任务，可参考以下方案配置模拟公司总部防火墙，以保障网络通信安全。

（1）网络连通性配置。如图 6-3 所示，模拟公司总部防火墙外部接口 outside，使用 IP 地址为 200.100.8.126/30；内部接口 inside，使用 IP 地址为 200.100.8.121/30。防火墙通过一个边界路由器连接到 Internet，该路由器内网接口使用 IP 地址为 200.100.8.125，连接 Internet 接口使用 IP 地址为 200.100.15.197。

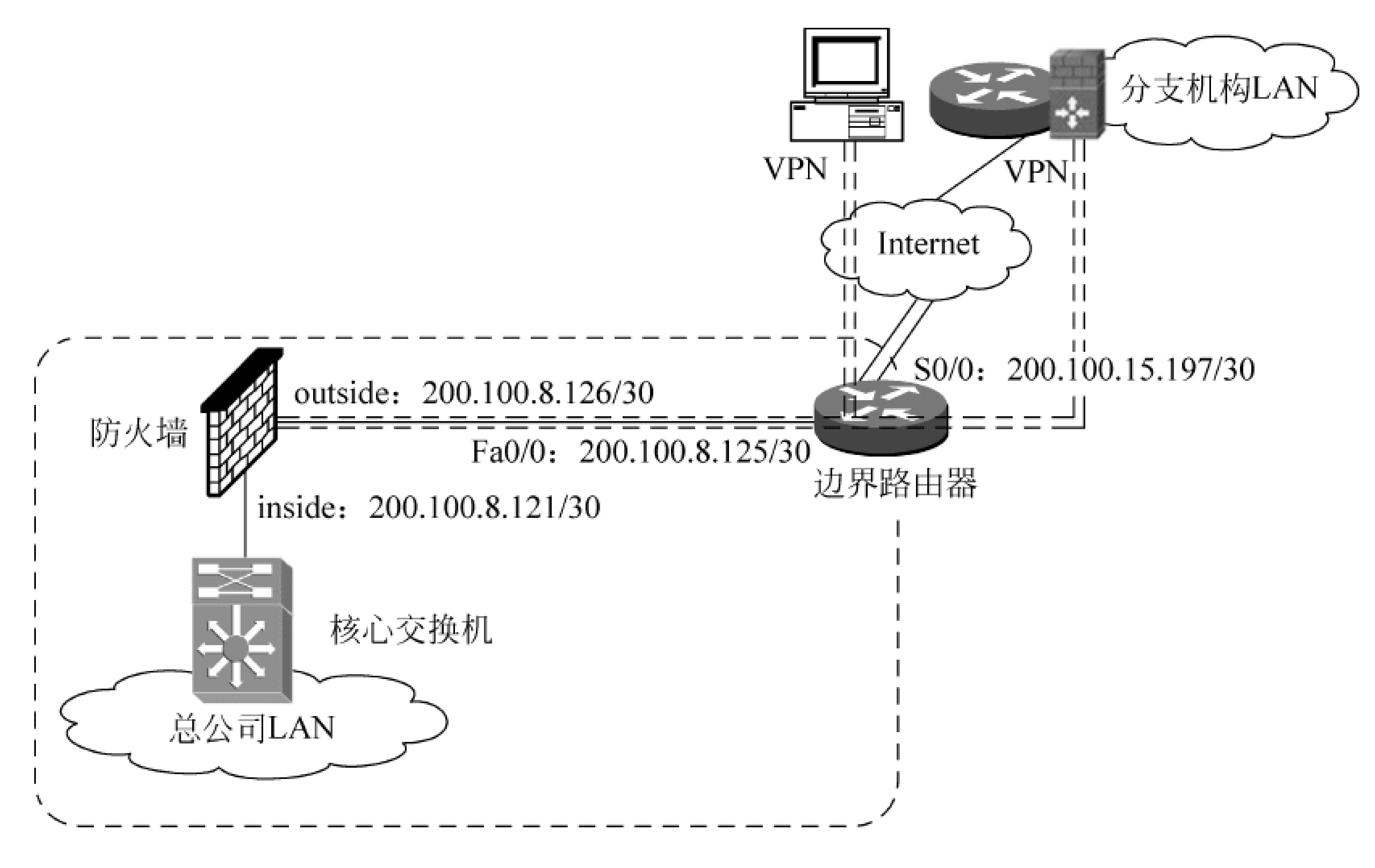


图 6-3　总部边界网络连通性

（2）配置访问控制，仅允许外部网络访问内部 Web 服务器 200.100.8.27/27，邮件服务器 200.100.8.28/27。

（3）根据防火墙默认访问规则，从防火墙外网到内网主动 TCP 连接是被默认禁止的，但从内网到外网的连接默认是不受限制的，所以使用防火墙默认模式即可满足要求。

（4）配置预共享密钥的站到站 VPN，以防火墙 outside 接口作为 VPN 对等体的本地地址，保障模拟公司总部与分支机构网络间通信，相应的 VPN 配置要求可参考表 6-7。

（5）配置远程访问 VPN，保障网管员能远程访问模拟公司总部网络内的网络设备。防火墙作为 VPN 服务器，其组策略配置内容如表 6-7 所示。

表 6-7　远程访问 VPN 组策略配置

组策略名	tg-rvpn
组策略类型	remote-access
组策略地址池名及范围	pool-rvpn：200.100.8.33～200.100.8.40
组策略中预共享密钥	每月随机生成更换

6.6　小结

相对于路由器，硬件防火墙使用专门的硬件进行网络安全通信处理，因此常被用于网络边界完成网络安全保障功能；要实现 Cisco PIX 防火墙网络连通性，必须配置网络接

口、路由、地址转换、ACL。Cisco PIX 防火墙与路由器在站到站 VPN 配置操作方面的主要不同有：需要在接口上启用 ISAKMP、需在全局配置模式下应用加密图。Cisco PIX 防火墙与路由器在远程访问 VPN 配置方面的主要不同有：需要在接口上启用 ISAKMP，组策略的配置又分为 general-attributes、ipsec-attributes 若干子项内容。

6.7 习题

1. 判断题：防火墙设备与路由器设备的区别在于，路由器设备上使用了专用硬件实现网络间访问控制。

2. 列举常见的 3 种防火墙类型及特点。

3. 判断题：代理防火墙的优点是只根据报头信息过滤报文，因此占用较少资源。

4. 根据 Cisco PIX 防火墙默认安全规则，下列哪些说法是正确的？(　　)

A. 为满足从内网对外提供公共网络服务的需求，需配置允许从 outside 接口入站的某些流量

B. 防火墙与路由器一样，只需为防火墙配置接口地址，并启用接口，就能实现内外网连通

C. 要能 ping 通防火墙的远端接口，需要使用 icmp permit any outside 命令

D. 从防火墙 inside 接口所连网络到 outside 接口所连网络的流量，默认是被允许的

E. 默认防火墙 dmz 接口与 outside 接口的安全级都为 0，则不需配置任何访问控制，从 outside 接口入站的流量就能被送到 dmz 接口

6.8 实训

6.8.1 防火墙网络连通性及访问控制配置

1. 实训组织

实训学时：100 分钟。

学生分组：2 人/组。

2. 实训目的

通过实训，熟练掌握防火墙网络连通性及访问控制配置操作。

3. 实训环境

(1) 安装有 Windows 系统、网络服务软件(例如 XAMPP)的 PC，每组 3 台。

(2) Cisco PIX 防火墙，每组 1 台。

(3) Cisco 路由器，每组 1 台。

(4) UTP 交叉电缆，每组 4 条。

(5) Console 电缆，每组 1 条。

注意保持防火墙为出厂配置。

4. 实训准备

按照图 6-4 所示连接网络设备，搭建实训环境。该网络拓扑为模拟公司总部网络简化而成，省略了部分与实训内容无关的网络设备。

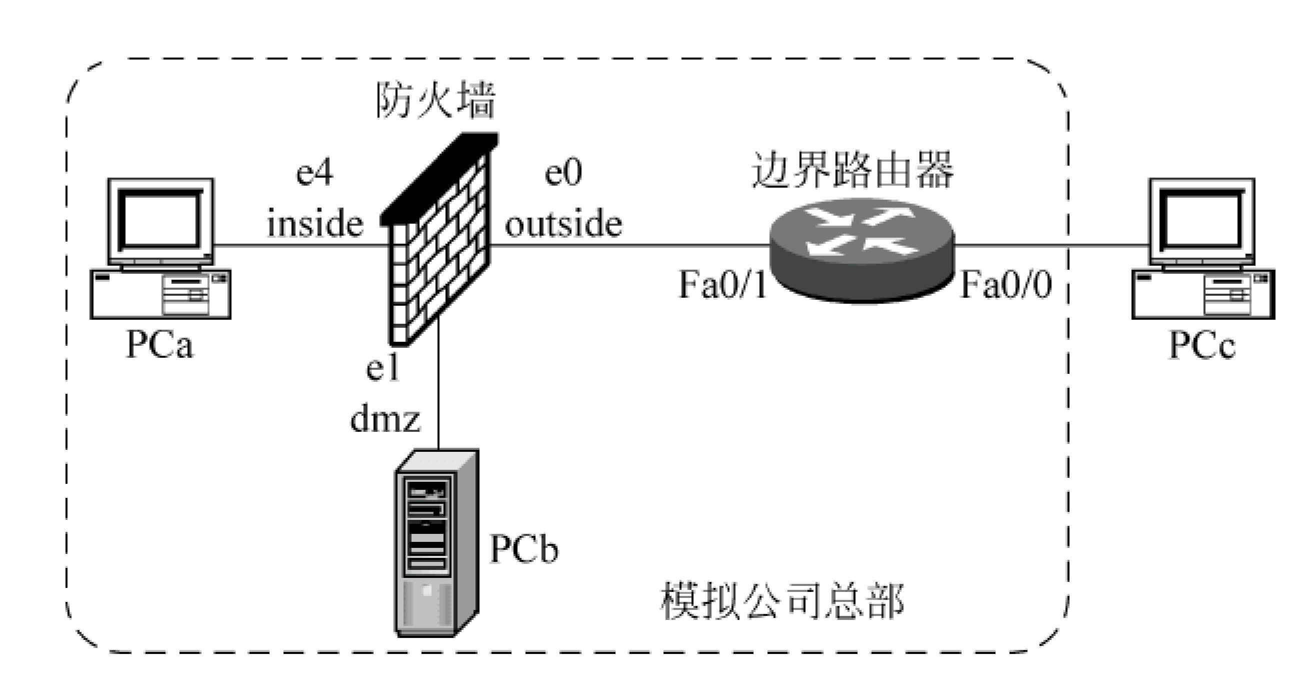


图 6-4 防火墙网络连通及访问控制配置实训拓扑

5. 实训内容

(1) 防火墙接口配置。

(2) 防火墙路由配置。

(3) 防火墙地址转换配置。

(4) 防火墙访问控制配置。

6. 实训指导

(1) 防火墙接口配置

按照表 6-8 所示，为实训网络中各接口配置 IP 地址。其中防火墙上的配置操作如下。

表 6-8 防火墙网络连通实训地址分配

接 口	IP 地址/网络前缀	网 关
PCa(模拟内网主机)	200.100.8.122/30	200.100.8.121/30
PCb(模拟 Web 服务器)	200.100.8.28/27	200.100.8.30/27
PCc(模拟外网主机)	200.100.15.198/30	200.100.8.121/30
防火墙 e0 接口(outside)	200.100.8.126/30	
防火墙 e1 接口(dmz)	200.100.8.30/27	
防火墙 e4 接口(inside)	200.100.8.121/30	
路由器 Fa0/0	200.100.8.125/30	
路由器 Fa0/1	200.100.15.197/30	

```
pixfirewall(config)# configure terminal
zbfw(config)# hostname zbfw
zbfw(config)# int erface e0
zbfw(config-if)# nameif outside
zbfw(config-if)# ip address 200.100.8.126 255.255.255.252
```

```
zbfw(config-if)# no  shutdown
zbfw(config-if)# interface  e1
zbfw(config-if)# nameif  dmz
zbfw(config-if)# ip  address  200.100.8.30  255.255.255.224
zbfw(config-if)# no  shutdown
zbfw(config-if)# interface  e4
zbfw(config-if)# nameif   inside
zbfw(config-if)# ip  address  200.100.8.121  255.255.255.252
zbfw(config-if)# no  shutdown
zbfw(config-if)# exit
```

（2）防火墙路由配置

在防火墙上配置 OSPF 路由协议，发布网络路由，其操作可如下进行。

```
zbfw(config)# router  ospf  1
zbfw(config-router)#  network  200.100.8.0  255.255.255.128  area  0
zbfw(config-router)#  exit
```

在防火墙上配置静态默认路由，默认网关为边界路由 Fa0/0 接口。

```
zbfw(config)#  route  outside  0.0.0.0  0.0.0.0  200.100.8.125
```

（3）防火墙地址转换配置

在防火墙上配置不进行地址转换，因为内网并未使用私有地址。

```
zbfw(config)#  nat  (inside)  0  0  0
zbfw(config)#  nat  (inside)  0  200.100.8.0  255.255.255.128
```

注意：以上两条命令中的第 1 个 0，意味着将不对后面定义的地址进行转换。第 1 条命令中的第 2 个 0，表示对所有本地网络(防火墙接口所在网络)不做地址转换，第 3 个 0 为子网掩码。

（4）防火墙访问控制配置

在防火墙上配置允许外部网络访问内部网络的 Web 服务器 200.100.8.27，并能使用 ping 测试网络连通性，其配置操作如下。

```
zbfw(config)# access-list  out2in  extended  permit  icmp  any  any
zbfw(config)# access-list  out2in  extended  permit  any  host  200.100.8.27  eq  80
zbfw(config)# access-group  out2in  in  interface  outside
```

配置完成后，测试是否从 PCc 访问 PCb 上的 Web 服务。

7. 实训报告

1. 简述 Cisco PIX 防火墙上配置网络连通性必需的步骤。

续表

2. 记录在防火墙上为接口配置 IP，但未配置接口名时，使用 show interface ip brief 命令查看到的结果。

3. 在防火墙上查看路由的命令为：________________________________。
记录防火墙上的路由。

4. 在不配置地址转换的情况下，配置访问控制允许 ICMP 流量。
从 PCa ping PCc：通 □　不通□
从 PCb ping PCc：通 □　不通□
从 PCc ping PCa：通 □　不通□

5. 在配置了允许 ICMP 流量的访问控制和 nat(inside)0 的情况下：
从 PCa ping PCc：通 □　不通□
从 PCb ping PCc：通 □　不通□
从 PCc ping PCa：通 □　不通□

6. 按内网使用私有地址 10.0.0.0/24 配置防火墙。写出各接口 IP。

接　口	IP 地址/网络前缀	网　关
PCa(模拟内网主机)		
PCb(模拟 Web 服务器)		
防火墙 e1 接口(dmz)		
防火墙 e4 接口(inside)		

7. 如果防火墙内网使用私网地址 10.0.0.0/24，则配置 PAT 将其私网地址转换为公网地址 200.100.8.116～200.100.8.119 的命令如下。

nat(________)　1　__________　__________
global(________)　__________　interface outside

6.8.2　防火墙预共享密钥站到站 VPN 配置

1. 实训组织

实训学时：200 分钟。
学生分组：2 人/组。

2. 实训目的

通过实训，熟练掌握防火墙与路由器间预共享密钥站到站 VPN 的配置操作。

3. 实训环境

(1) 安装有 Windows 系统、网络服务软件(例如 XAMPP)的 PC，每组 3 台。
(2) Cisco PIX 防火墙，每组 1 台。
(3) Cisco 路由器，每组 1 台。

(4) UTP 交叉电缆,每组 4 条。

(5) Console 电缆,每组 1 条。

注意保持所有的网络设备为出厂配置。

4. 实训准备

按照图 6-5 所示模拟公司总部局域网简化拓扑示意图搭建实训环境。

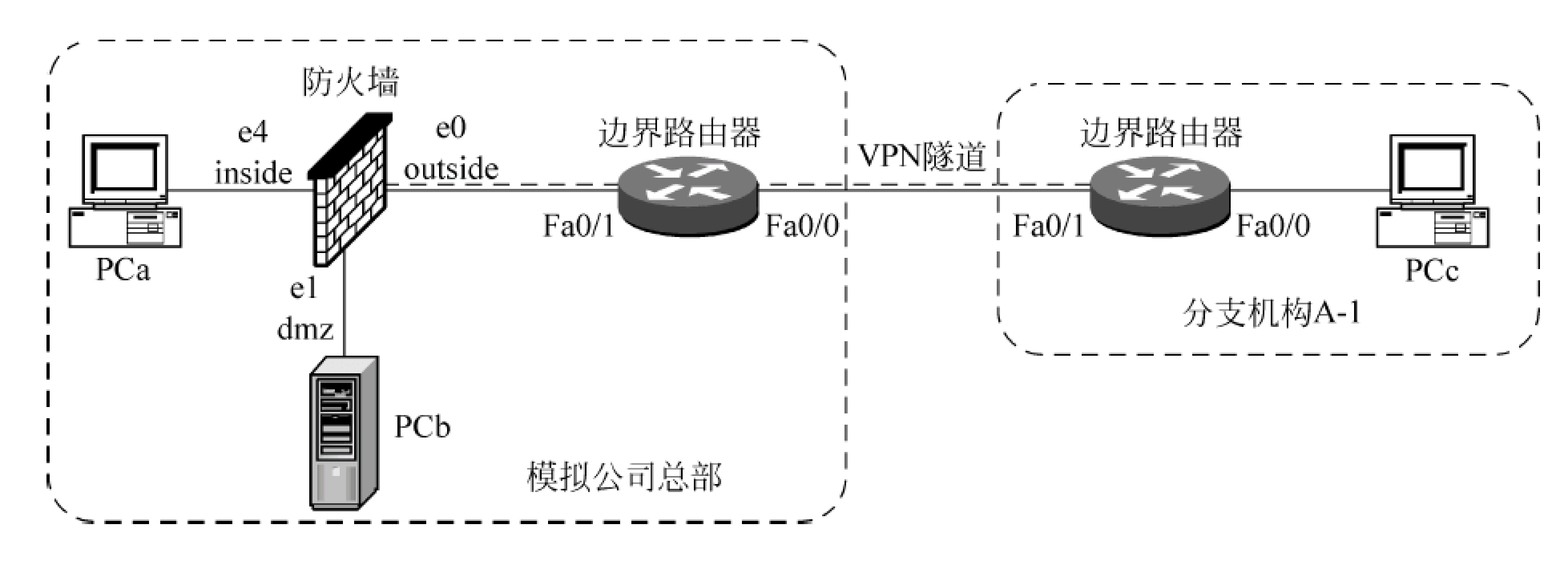


图 6-5 预共享密钥站到站 VPN 配置实训拓扑

5. 实训内容

本实训在模拟公司总部的行政管理网络 200.100.8.128/25 与分支机构 A-1 网络 200.100.14.0/24 间搭建 VPN 安全隧道。本实训任务内容如下。

(1) 防火墙网络连通性的配置。

(2) 路由器预共享密钥站到站 VPN 配置。

(3) 防火墙预共享密钥站到站 VPN 配置。

6. 实训指导

(1) 网络连通性配置

参照 6.8.1 小节配置防火墙网络连通性,完成整个实训网络的网络连通性配置。该网络中 IP 地址分配如表 6-9 所示。

表 6-9 防火墙 VPN 实训地址分配

接　　口	IP 地址/网络前缀	网　　关
PCa(模拟内网主机)	200.100.8.129/25	200.100.8.254/30
PCb(模拟 Web 服务器)	200.100.8.28/27	200.100.8.30/27
PCc(模拟外网主机)	200.100.14.254/24	200.100.14.1/24
防火墙 e0 接口(outside)	200.100.8.126/30	
防火墙 e1 接口(dmz)	200.100.8.30/27	
防火墙 e4 接口(inside)	200.100.8.254/30	
总部路由器 Fa0/0	200.100.15.197/30	
总部路由器 Fa0/1	200.100.8.125/30	
分支路由器 F0/0	200.100.14.1/24	
分支路由器 F0/1	200.100.15.198/30	

（2）路由器预共享密钥站到站 VPN 配置

参考第 5 章路由器上预共享密钥站到站 VPN 配置方法配置分支机构路由器。参考操作如下。

```
a1(config)# crypto isakmp policy 1
a1(config-isakmp)# authentication pre-share
a1(config-isakmp)# hash sha
a1(config-isakmp)# group 2
a1(config-isakmp)# encryption 3des
a1(config-isakmp)# exit
a1(config)# crypto isakmp key 123 address 200.100.8.126
a1(config)# crypto ipsec transform-set ts-rvpn esp-3des esp-md5-hmac
a1(cfg-crypto-trans)# exit
a1(config)# ip access-list extended eacl-vpn
a1(config-ext-nacl)# permit ip 200.100.14.0 0.0.0.255 200.100.8.128 0.0.0.127
a1(config-ext-nacl)# exit
a1(config)# crypto map map-vpn 1 ipsec-isakmp
a1(config-crypto-map)# set peer 200.100.8.126
a1(config-crypto-map)# set transform-set ts-rvpn
a1(config-crypto-map)# match address eacl-vpn
a1(config-crypto-map)# exit
a1(config)# interface f0/0
a1(config-if)# crypto map map-vpn
a1(config-if)# exit
```

（3）防火墙预共享密钥站到站 VPN 配置

注意：为能使防火墙与路由器间使用 ISAKMP 进行协商，使用 ESP 报文传输通信数据，需在防火墙上配置 ACL，使来自分支机构的 ISAKMP、ESP 流量不被过滤掉，此类流量在路由器上也应被放行。

```
zbfw(config)# access-list out2in extended permit udp host 200.100.15.198 host
200.100.15.197 eq 500
zbfw(config)# access-list out2in extended permit udp host 200.100.15.198 eq 500
host 200.100.15.197
zbfw(config)# access-list out2in extended permit esp host 200.100.15.198 host
200.100.15.197
zbfw(config)# isakmp policy 1
zbfw(config-isakmp-policy)# authentication pre-share
zbfw(config-isakmp-policy)# hash sha
zbfw(config-isakmp-policy)# group 2
zbfw(config-isakmp-policy)# encryption 3des
zbfw(config-isakmp-policy)# exit
zbfw(config)# isakmp enable outside
zbfw(config)# isakmp key 123 address 200.100.15.198 netmask 255.255.255.252
zbfw(config)# crypto ipsec transform-set ts-rvpn esp-3des esp-md5-hmac
zbfw(config)# access-list eacl-vpn extend permit ip 200.100.8.128 255.255.255.128
200.100.14.0 255.255.255.0
zbfw(config)# crypto map map-vpn 1 ipsec-isakmp
```

```
zbfw(config)# crypto map map-vpn 1 set peer 200.100.15.198
zbfw(config)# crypto map map-vpn 1 match address eacl-vpn
zbfw(config)# crypto map map-vpn 1 set transform-set ts-rvpn
zbfw(config)# crypto map map-vpn interface outside
```

(4) 检查网络连通性和 VPN 安全隧道

配置完成后，在 PCa 上 ping PCc，并用 show 命令在防火墙上检查 VPN 安全隧道能否建立起来。

7. 实训报告

1. 记录在分支机构路由器上的网络连通性配置命令。
2. 记录在防火墙上的网络连通性配置命令。
3. 在配置 VPN 前，从 PCa 上 ping PCc：通 □ 不通□ 在配置 VPN 后，从 PCa 上 ping PCc：通 □ 不通□
4. 记录配置 VPN 并从 PCa 上 ping PCc 后，在防火墙上使用 show crypto isakmp sa 命令的输出结果。
5. 记录配置 VPN 并从 PCa 上 ping PCc 后，在防火墙上使用 show crypto ipsec sa 命令的输出结果。

第 7 章

网络管理技术

本章任务：根据工程任务安全需求分析，解决计算机网络管理问题。

必备知识：(1) 网络管理体系架构。

(2) SNMP 协议。

(3) 网络配置管理。

(4) 网络故障管理。

(5) 网络安全管理。

(6) 网络性能管理。

(7) 网络计费管理。

学习目标：完成模拟公司总部局域网的网络管理任务。

7.1 模拟公司网络管理任务分析

由于模拟公司大部分生产、办公系统依赖于公司的计算机网络，因此对网络进行有效管理，保障网络安全、可靠、高效运行非常重要。模拟公司网络管理任务主要包括以下内容。

(1) 在相关网络管理软件协助下，及时了解网络拓扑变化，包括网络内路由器、三层交换机、接入层交换机之间，与其他设备之间的物理连接关系，局域网划分、VLAN 划分等。

(2) 在相关网络管理软件协助下，及时检测广域网线路各条线路的流量，统计过去任何一段时间，任何一条线路的输入/输出、总流量以及丢包率、错包率；以实时更新的流量统计方式对网络流量状况进行监测；能统计各线路丢包率、错包率，为线路性能的分析提供科学依据。

(3) 在相关网络管理软件协助下，及时发现网络故障发生点。记录网络设备、线路、终端、病毒、非法入网、违规操作、相关告警设置等各种严重和一般告警信息。

(4) 在相关网络管理软件协助下，进行设备的配置管理。

(5) 在相关网络管理软件协助下，进行日志管理，分门别类记录网络的各种故障；对网络的各类运行情况进行统计，掌握网络动态。

(6) 在相关网络管理软件协助下，进行安全管理，例如对使用 Internet 线路的网络连接使用加密技术进行保护，定期对网络进行安全审计等。

7.2 网络管理技术概述

7.2.1 网络管理模型

网络管理内容繁杂，涉及计算机网络的各个方面，因此针对网络管理定义的参考模型、技术等为数众多。其中最为知名的是 ISO 的 FCAPS 模型，如图 7-1 所示，它将网络管理分为故障管理(Fault Management)、配置管理(Configuration Management)、记账管理(Accounting Management)、性能管理(Performance Management)、安全管理(Security Management)5 个方面。

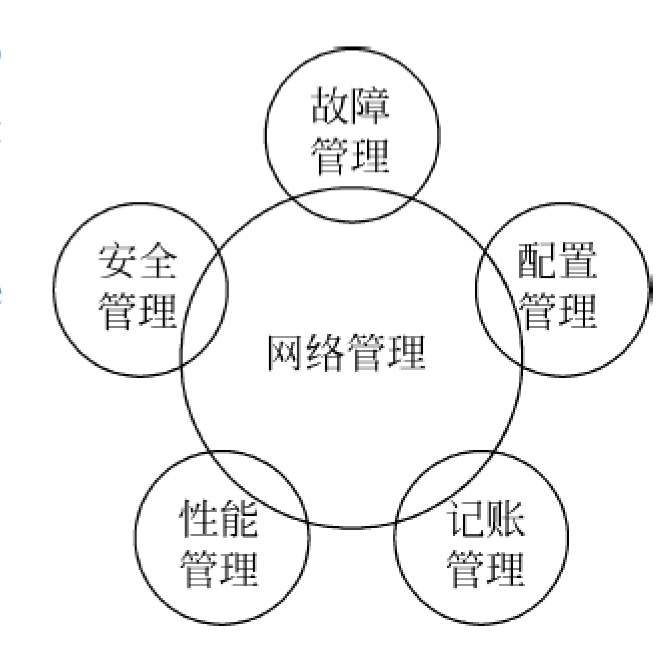


图 7-1 网络管理体系结构

(1) 故障管理

故障管理对网络中故障进行检测、隔离、报告和修复。故障管理的目标是保证计算机网络组件的稳定性、可用性和可服务性(Reliability、Availability and Serviceability, RAS)。故障管理包括以下功能。

- 检测被管对象的差错现象，接收被管对象的差错事件报告(也称故障单，Trouble Ticket)。
- 执行诊断测试、确定故障位置和性质。
- 当存在备用设备或迂回路由时，提供新的网络资源用于服务。
- 通过设备的维护或更换等措施进行修复。
- 维护差错日志文件，记录差错信息，分析故障原因。

(2) 配置管理

网络中每台设备的状况、功能及连接关系和工作参数等被称为网络配置，网络配置反映网络的状态。网络配置随着网络规模的变化、设备的更替，需要经常调整。

配置管理提供了标识、收集、更改网络配置数据的功能，目的是为了实现网络的最优化服务功能。网络配置管理功能包括以下内容。

- 收集网络配置信息。
- 修改网络配置信息。
- 安装软件。
- 存取配置信息。
- 发现和显示网络的拓扑结构。
- 生成配置报告。

(3) 记账管理

记账管理用来度量网络资源的使用情况，目的是控制和监测各类网络服务的费用和成本。记账管理对公共商业网络尤为重要，如公用电信网。记账管理功能一般包括以下

内容。

- 记录用户使用网络资源的情况和计算费用。
- 统计网络利用率等效益数据，为网络运营部门提供制定资费政策的依据。

这些管理工作的目的是使网络能正常高效地运行，使网络资源得到更加有效的利用。这些管理能够有效地维护网络的正常运行，当网络出现故障时能及时报告和处理，并协调、保持网络系统的高效运行。

（4）性能管理

性能管理主要是监测网络的性能，持续地评价网络的性能指标，验证网络的服务水平，找出已经发生或潜在的问题，形成网络性能变化的趋势，为网络管理提供决策依据，将故障排除在影响服务之前。

性能管理的主要功能是以网络性能为准，收集、分析和调整被管对象的状态，其目的是保证网络提供可靠、连续的服务。网络性能管理一般包括以下内容。

- 从被管对象中收集、统计与性能有关的数据，并产生相应记录。
- 分析性能信息，检测性能故障，产生性能告警等报告。
- 预测性能的长期变化趋势。
- 控制被管对象，保证网络的性能指标。

（5）安全管理

安全管理主要用于保护网络资源的安全，安全管理功能是网络管理的关键管理功能之一，只有建立了可靠的安全管理措施，才能做到有效地保护国家、企业和个人的机密，使网络能够安全运行。

网络安全管理包括进网安全防护，限制非法入侵者入网；应用软件访问的安全防护，检查用户访问软件的权限；网络传输信息的安全防护，对网络传输信息的加密、防“窃听”、防破坏和篡改等。

安全管理一般是通过设置权限、口令等判断非法入侵者（越权操作）。当检测到非法入侵者后，分别采取积极或消极行动予以处理。积极行动包括发出告警信息，同时拒绝入侵者的访问；消极行动则是收集有关数据产生报告，交网管中心的安全事务处理进程分析、记录、存档，并根据情况给予取消权利、发出警告信息等处理。

网络安全管理完成的功能一般包括以下内容。

- 安全措施信息的管理，如用户口令、密钥、访问权限的管理，并根据安全措施信息判断非法操作，拒绝非法操作。
- 安全审查，检查网络各种潜在安全漏洞。
- 安全报告，对影响网络安全事件进行记录，形成报告。
- 网络操作事件的记录，记录用户登录、退出，记录涉及网络安全的网络操作，以便进行安全追查等事后分析。

7.2.2　网络管理体系结构

如图 7-2 所示为目前常用的一种网络管理体系结构，主要包括 4 部分：网络管理实体、网络管理协议、网络管理代理、管理信息库。

网络管理实体即网络管理系统进程，它向运行在各网络设备上的网络管理代理程序

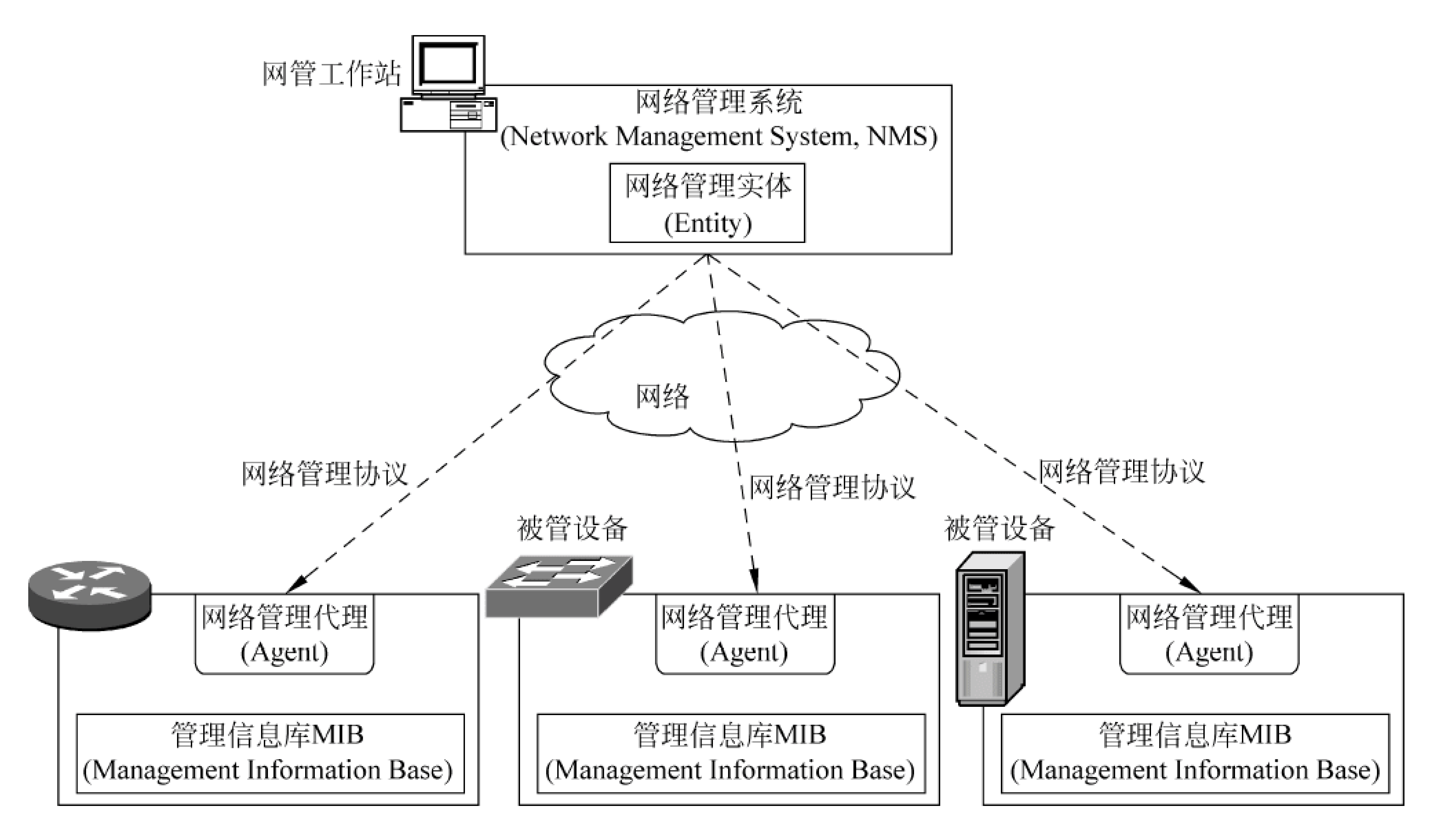


图 7-2 网络管理体系结构

发出指令，对各种网络设备、网络资源进行监控和控制。

网络管理协议是网络管理实体与网络管理代理程序间进行通信所遵守的规则和约定。

管理信息库是被管理对象的信息集合。

网络管理代理是驻留在网络设备、网络资源等网络实体上的，被网络管理实体控制的进程，它接收网络管理实体发来的指令，从管理信息库中读取或修改被管理对象的各种配置信息，并能以通知的形式向网络管理实体报告被管理对象上发生的重要事件。

7.2.3 SNMP 协议

ISO 的 CMIP/CMIS（Common Management Information Protocol and Common Management Information Services，通用管理信息协议和通用管理信息服务）和 IETF 的 SNMP（Simple Network Management Protocol，简单网络管理协议）是目前两种主要的网络管理协议。其中 CMIP/CMIS 较为有限地应用在基于 OSI 的网络中；而 SNMP 则广泛应用在数据网络，尤其是 TCP/IP 网络中。

SNMP 网络管理协议的基本工作原理是使管理者通过轮询被管代理，和被管代理自动发给管理者的陷阱信息，来设置一些被管对象的属性和监控一些网络事件的发生，从而达到网络管理目的。SNMP 是基于 TCP/IP 协议的应用层协议，采用无连接的传输层协议 UDP 传送网络管理报文。采用 SNMP 协议的网络管理系统，网络管理实体之间的通信不需建立连接，对报文能否正确到达不做检验，从而降低了系统开销。

SNMP 的结构分为 SNMP 管理者（SNMP Manager）和 SNMP 代理（SNMP Agent）。每一个支持 SNMP 的网络设备中包含一个 SNMP 代理，它随时记录网络设备的各种情况。网络管理进程通过 SNMP 协议查询或修改代理所记录的信息。

SNMP 的工作原理非常简单，在 SNMP 的管理者（运行网络管理系统的计算机）和 SNMP 代理（被管设备、实体）之间实时传递网络管理信息（PDU）。SNMP 提供的管理操作如下。

- 管理进程从代理处获取被管对象的信息。
- 管理进程通过代理设置或修改被管对象的属性。

SNMP 的网络管理操作采用的是轮询管理策略和事件管理策略。当网络管理进程需要了解某个设备的状态时，通过 SNMP 发送一个“读请求”的协议数据单元，该被管代理收到 SNMP 的数据报后，回答一个“响应”数据报，把管理进程需要的信息送给管理进程；当网络管理进程需要改变远地某个设备的状态时，例如把一个路由器的某个端口状态由 Disable 变为 Enable，开放一个路由器端口，增加一条路由设置时，管理员通过 SNMP 发送一个“设置请求”数据报给被管对象的代理，由被管代理完成设备状态的设置。

在 SNMP 中，被管对象的当前状态符合某种预先设定的状态时，即发生了某种特定的事件时，它会向管理进程主动发出一种协议单元，主动向管理者报告自己状态的变化，这种协议单元称作陷阱报文。陷阱报文在智能网络管理中是非常重要的，当网络出现故障时，管理进程可以根据陷阱报文进行诊断和故障处理。

在一个网络中只有一个管理者，其他都是被管代理时，称为集中式网络管理。在网络相当庞大时，集中式管理就非常困难。SNMP v2 中增加了管理者之间的通信功能，即在一个网络中，可以有多个管理者，可以实现分层多级管理。在分层多级网络管理中，可以按照层次设置多个管理者，高层管理者只管理下属的一些管理器，最低层管理者才管理具体被管对象。

当网络中有多个管理者时，被管代理不能接收非法管理者的管理操作，以保证整个网络的正常运行，为网络提供一定的安全性。为了使 SNMP 代理拒绝非法管理者的网络管理报文，在 SNMP 中使用了共同体的概念（Community），在 SNMP 管理者和 SNMP 代理之间设置一个共同体名字，只有具有相同共同体名字的管理者才能对 SNMP 代理进行管理，当检查管理报文中共同体名不符时，SNMP 代理将丢弃管理报文。另外在 SNMP 代理上还可以设置管理者的 IP 地址清单，通过 IP 源地址判别是否是合法的管理者。一个 SNMP 代理可以同时属于多个共同体。

7.2.4　MIB 与 SMI

MIB 是被管对象信息的集合，表示网络中各种网络设备、网络资源的状态，是网络管理系统实现的基础。但实际上，网络中并不存在一个完整的管理信息库 MIB，MIB 是和被管代理一起存在于具体的被管对象上，如 Router、Firewall、Switch 等，由被管对象上的代理进程维持其和物理实体的一致性，网络管理进程通过被管代理对 MIB 进行访问和控制。

为规范 MIB 中网络管理信息的表示方式，SNMP 协议网络管理体系中由 RFC1155 定义了“管理信息结构（Structure of Management Information，SMI）”，即各种被管对象表示、命名的方法。

在 SMI 中，使用“抽象语法符号 1（Abstract Syntax Notation One，ASN.1）”的描述

形式，定义了网络中 6 个主要的被管对象类型：网络地址、IP 地址、时间标记、计数器、计量器和非透明数据类型。SMI 中还定义了表示管理信息的标准方法，规定每个对象都有 3 个属性：名字、语法和编码。

为了能够在 MIB 中唯一标识某种对象，SMI 采用了 ASN.1 树形结构来表示被管理对象的信息，如图 7-3 所示。每个 MIB 对象由对象标识符(Object Identifier，OID)唯一标识，OID 是一组以“点”分隔的字符串或整数，它指示了该被管对象在树形结构中的位置。例如，Cisco 网络设备上 VLAN 信息的 MIB OID 为 1.3.6.1.4.1.9.5.1.9.3。

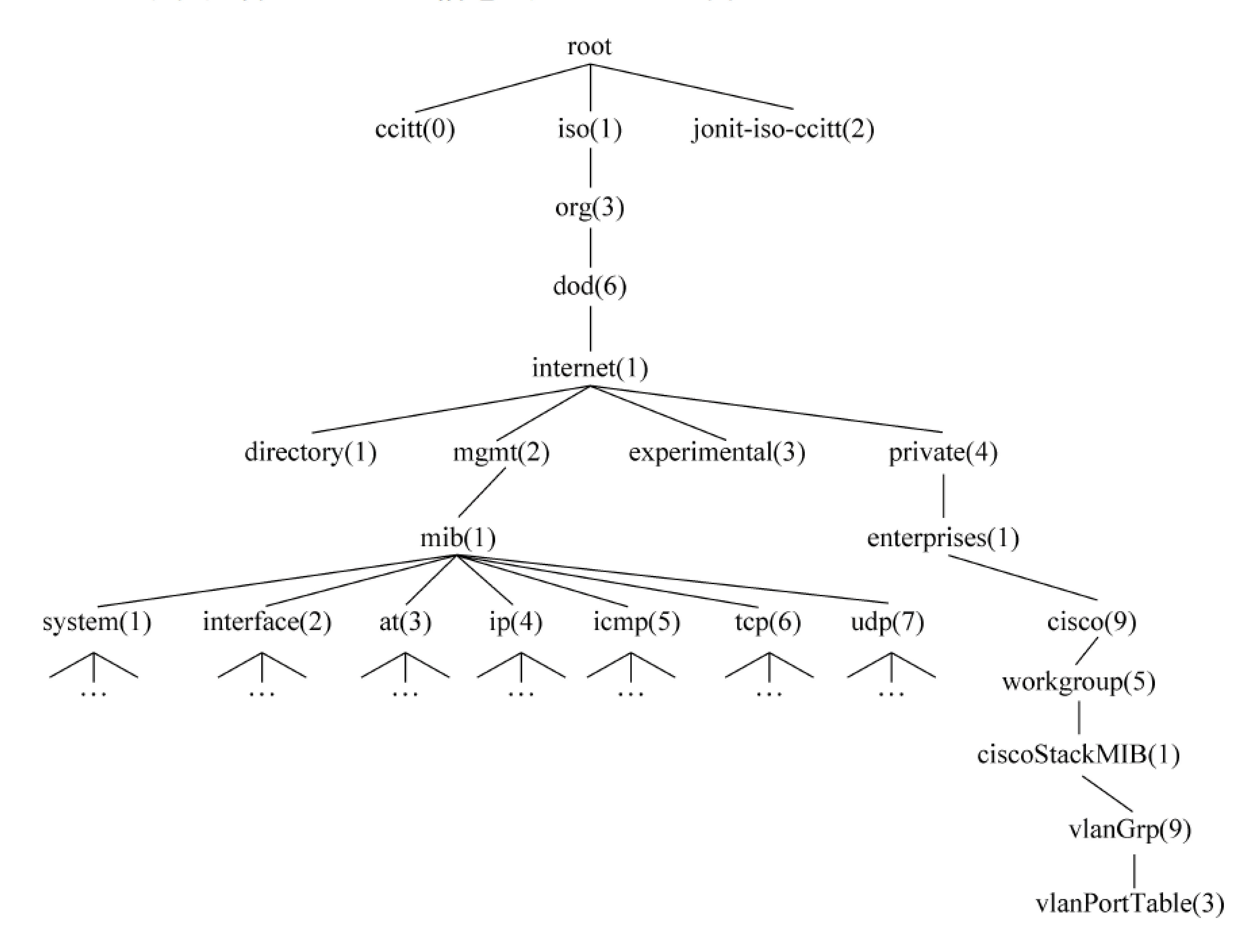


图 7-3 SMI 中的 OID

7.2.5 网络管理工具

网络管理工具是指能够协助网络管理员采集、分析网络管理数据，调整网络配置的软硬件。目前常用网络管理工具种类繁多，功能、规模相差很大。例如，从功能上分类，有能提供网络管理 5 项功能的网络管理平台，如 HP OpenView，也有只能提供络部分管理功能的网络管理软件，如进行网络性能监控的 PRTG，甚至是只能检测一项网络状态的命令行工具，如 ping。另外，网络管理工具可能是一个能够管理各种网络设备、资源的通用网络管理软件，如 HP OpenView、IBM Tivoli，也可以是网络设备厂商专门为其网络设备制作的网络管理软件，如 Cisco 的 CiscoWorks 系列网络管理软件。

网络管理员在选择网络管理工具时，需要根据网络管理需求、所能实现的网络管理成本、网络设备所能支持的网络管理功能等各方面因素进行考虑。

7.3 网络配置管理

网络配置管理包括对网络中网络设备、网络服务等网络中各组件配置信息的管理、修改和状态监控。限于篇幅和内容，有关网络服务配置管理可参见本系列教材中《网络操作系统》一书，本书不再赘述。

1. 收集网络配置信息

网络设备配置信息保存方式及收集手段如表 7-1 所示。

表 7-1 收集网络配置信息

网络配置信息	收 集 方 式
配置文件	使用 FTP、TFTP 工具传送配置文件
网络节点配置、状态信息	使用 Telnet、SSH 远程登录网络设备查看配置、状态信息
MIB	使用网络管理软件通过 SNMP 代理收集配置信息

采集、保存路由器、交换机配置文件以及使用远程访问方式登录网络节点查看网络配置的操作可参考本系列教材中《计算机网络集成技术》一书；使用网络管理软件通过 SNMP 代理收集配置信息的方式，参见本书 7.6.2 小节。

需要注意的是，通过网络访问网络设备配置信息时，建议为网络设备配置专门的管理地址。同时，为保证网络设备管理地址所在接口的稳定性，一般在路由器上使用 Loopback 接口、在交换机上使用管理 VLAN 虚接口作为网络设备管理地址所在的接口。

在 Cisco PIX 防火墙上对使用 Telnet 远程访问防火墙进行了严格限制。虽然防火墙任何接口都可以配置用来访问防火墙，但 Cisco PIX 防火墙要求来自外部接口的 Telnet 流量需要经过 IPSec 的保护。

在 Cisco PIX 防火墙上配置启用 Telnet 的操作步骤如表 7-2 所示。

表 7-2 Cisco PIX 防火墙 Telnet 访问配置步骤

序 号	操 作	相 关 命 令	必要
步骤 1	指定可以访问防火墙的主机	**telnet**	是
步骤 2	指定 Telnet 访问使用的口令	**passwd**	是
步骤 3	指定 Telnet 会话空闲时间	**telnet timeout**	可选
步骤 4	检查 Telnet 配置	**show running-config**	可选
步骤 5	管理 Telnet 会话	**who** **kill**	可选

(1) 指定可以访问防火墙的主机

在 Cisco PIX 防火墙上，指定可以访问防火墙主机的操作为在全局配置模式下输入：

telnet 主机(网络)IP 地址或主机名 子网掩码 接口

参数“主机(网络)IP 地址或主机名”及“子网掩码”用于定义哪些主机或网络可以使

用 Telnet 方式访问防火墙。注意，Cisco PIX 防火墙最多可支持 16 个主机或网络 Telnet 访问。

参数“接口”用于定义 Telnet 访问来自于防火墙的哪个接口。

例如，如下命令将定义网络 192.168.1.0 能够通过 inside 接口访问防火墙。

```
pixfirewall(config)# telnet  192.168.1.0  255.255.255.0  inside
```

(2) 指定 Telnet 访问使用的口令

在 Cisco PIX 防火墙上，指定 Telnet 访问使用的口令的操作为在全局配置模式下输入：

```
passwd  口令
```

(3) 指定 Telnet 会话空闲时间

当会话空闲时断开连接，可以节省防火墙资源。在 Cisco PIX 防火墙上，指定 Telnet 会话空闲时间的操作为在全局配置模式下输入：

```
telnet  timeout  空闲时间
```

参数“空闲时间”单位为秒，默认值为 5。

(4) 管理 Telnet 会话连接

在 Cisco PIX 防火墙上可以使用 who 命令检查有哪些主机登录到防火墙上，并可以使用 kill 杀掉已经连接到防火墙的 Telnet 连接。其操作如下。

```
pixfirewall# who
          0: 192.168.1.1
pixfirewall# kill  0
pixfirewall# who
```

使用 who 命令可以查看 Telnet 连接的连接 ID，在杀掉 Telnet 连接时，需在 kill 命令后使用连接 ID 指定杀掉哪个连接。

2. 修改网络配置信息

修改网络节点的配置信息，可以通过两种方式进行。一种是通过远程访问，例如 Telnet、SSH；另一种是通过网络管理软件，例如 HP OpenView 等。

一般在大型网络中，才会选择使用通用网络管理软件来对网络设备进行配置修改管理；大部分网络会选择使用网络设备配套的网络管理软件对其进行管理，例如 Cisco 路由器的 SDM 软件，Cisco PIX 防火墙的 PDM 软件，Cisco 交换机的 Lan Manager；另外很多网络管理员仍然习惯使用 Telnet 或者 SSH 远程登录网络设备，配置网络设备。

3. 发现和显示网络的拓扑结构

网络拓扑管理是将网络设备间的连接关系以图形方式显示出来，帮助网络管理员更好管理网络。网络拓扑管理一般通过网络拓扑管理工具实现。专业的网络管理软件中一般都会设置网络拓扑管理功能。另外也有一些免费的网络拓扑发现工具，例如可以在局域网中使用的 LanTopolog，如图 7-4 所示。

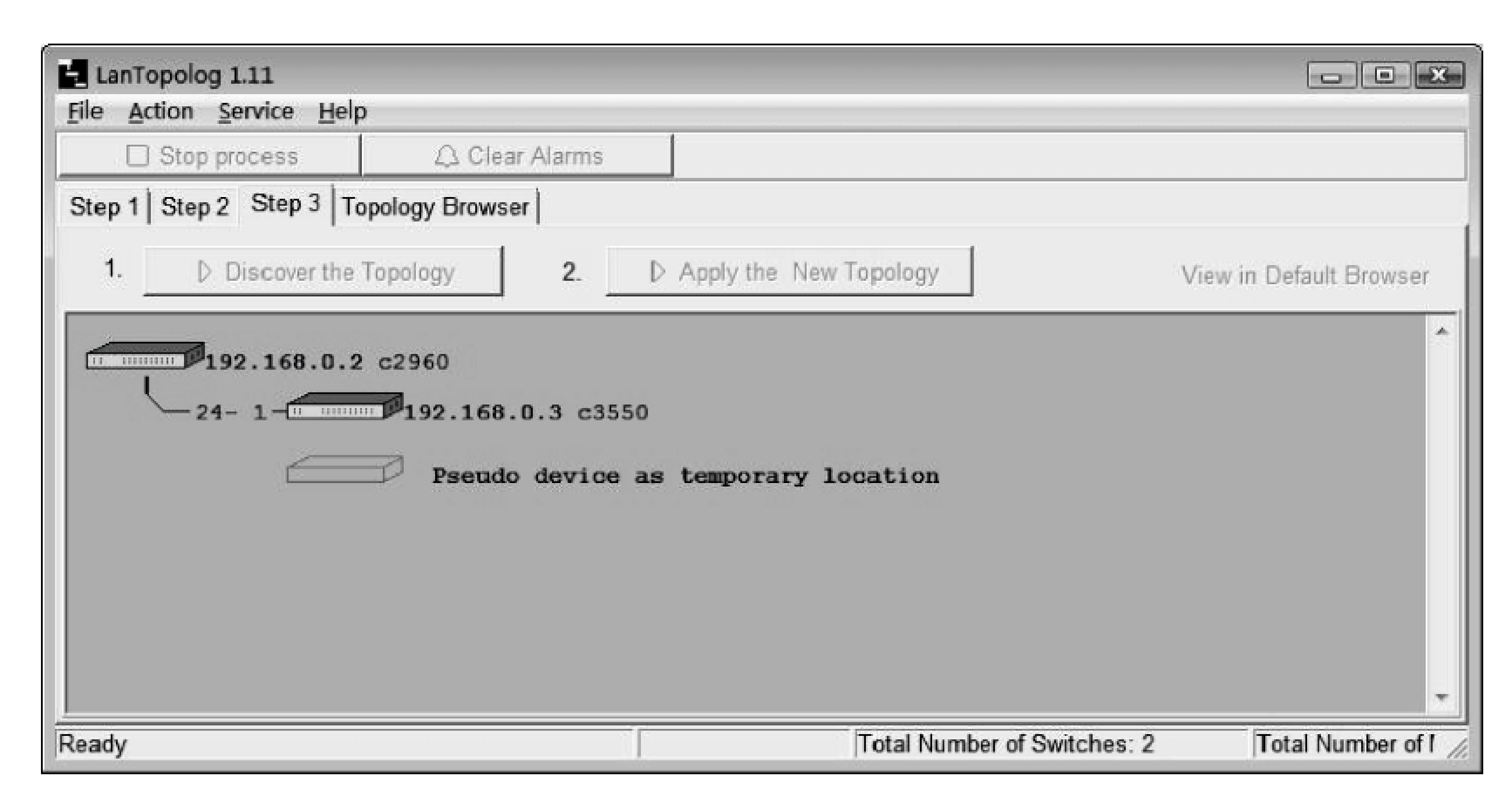


图 7-4　网络拓扑发现软件示例

7.4　网络故障管理

网络故障管理流程如图 7-5 所示。当发现网络出现故障时，需先收集网络故障有关数据；然后根据这些数据对网络故障原因进行分析，定位故障点、故障层次；接着应根据故障分析结果，制定故障排除方案，并对方案进行测试；如果方案经过测试可行，则可以按照方案实施排除故障；如果实施故障排除方案后还不能排除故障，则应回退重新收集故障数据，进行故障排查过程。

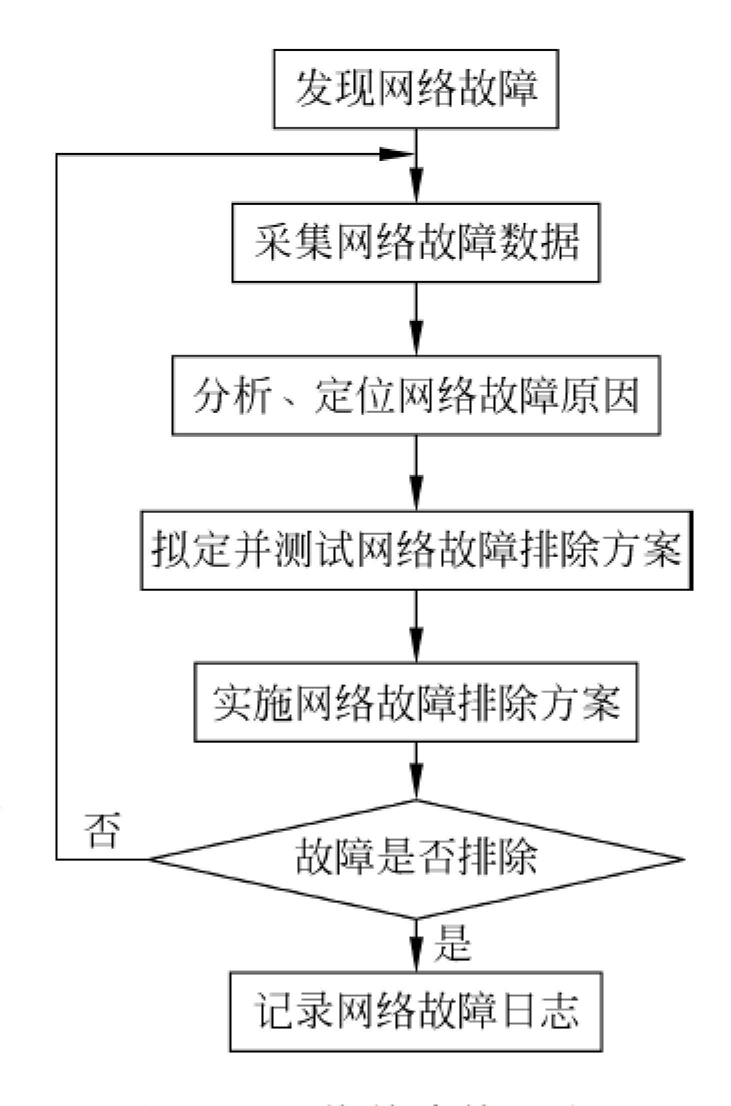


图 7-5　网络故障管理流程

7.4.1　网络故障监测

网络管理中监测网络故障的方式有两种：异步告警、主动轮询。异步告警是指网络设备在发生故障后，主动向网络管理系统发出警报；主动轮询是指由网络管理软件定期查询网络节点状态。

7.4.2　网络故障分析定位

网络故障分析定位的常用方法有：分层法、分段法、替换法和比较法。

1. 分层排查网络故障

计算机网络是基于 OSI 分层模型构建起来的。根据不同网络层次的功能特点，可以使用相应层次的检测工具，自上而下或自下而上逐层进行测试检查，以定位故障点。

自上而下的检查方法是指先从 OSI 模型的应用层开始检查故障原因，然后逐层向下检查。例如，当发现网络服务不能访问时，可按图 7-6 所示检查各层网络组件是否存在问题。

自下而上排除法是指从物理层开始，逐层向上排查网络故障的方法。

一般情况下，如果根据故障现象已能够大致判断出网络层次范围时，可采用自上而下方法进行排查；当网络故障原因复杂，难以快速判断层次时，可采用自下而上的方法进行排

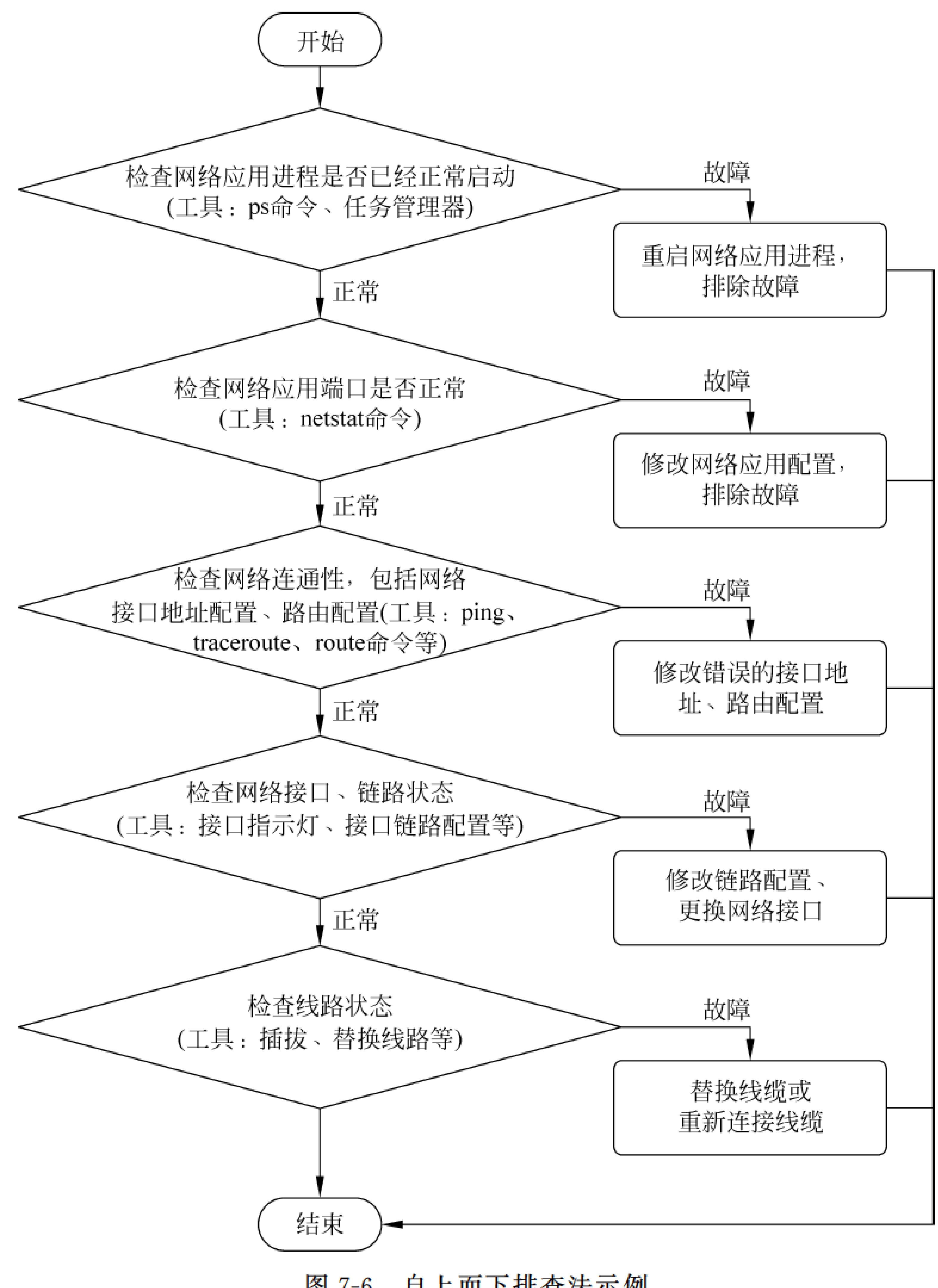


图 7-6　自上而下排查法示例

查，由于网络上层通信需依赖下层提供的服务，所以使用该方法能够准确定位网络故障层次。

2．分段排查网络故障

分段排查网络故障是指以网络拓扑为参考，沿网络连接，逐段检查网络故障点的故障排除方法。分段排查时，还可使用"二分法"提高检查效率。

例如，当要排查出向网络发送大量病毒包的主机时，网络管理员常用的一种方法就是逐个断掉网络上主机的网络连接，直到发现网络病毒包大量减少时，则可判定被断掉网络连接的主机被病毒入侵了。

3．替换法排查网络故障

替换法是指用另外的网络组件替换当前网络组件，以检测当前网络组件是否存在问题的故障排查方法。例如，排查电缆故障时，可以使用另外的线缆替换当前线缆，以检查

原电缆是否出现了问题。

4. 比较法排查网络故障

比较法是指将故障点与其他相似的网络环境进行比较，以帮助分析故障发生原因。例如，当网络中某个节点无法连接到网络时，可检查网络中其他节点情况，如果仅该节点存在网络连通性问题，则可以认为问题出在该节点上。

7.5　网络安全管理

7.5.1　网络安全管理概述

1. 网络安全管理目标和对象

网络安全管理目标可归纳为如下 5 个方面。

（1）机密性：网络上传输的信息受到保护，只能被指定用户读取。

（2）完整性：网络能保证信息通过网络传输时不被破坏、篡改。

（3）可用性：网络能够提供稳定、持续的网络服务，得到授权的用户可以按照指定的途径访问网络资源。

（4）抗抵赖性：网络提供事件记录、身份认证等功能，使网络实体无法抵赖已经发生的网络行为。

（5）可控性：网络具有可管理性，能够被监测和控制。

网络安全管理涉及网络系统的各个方面，包括物理环境安全、人员安全、访问控制、备份与恢复等。网络安全管理的对象包括网络系统中的主机、网络设备、网络链路线路、使用网络的个体、网络赖以存在的物理环境、网络配置信息、软件、数据等各个方面。

2. 网络安全管理工作流程

网络安全管理的工作流程如图 7-7 所示。进行网络安全管理的第 1 步，是根据业务需求明确网络安全目标，制定网络安全策略；然后根据网络安全策略，对网络进行安全配置；在实施了必要的安全防护措施后，应使用网络安全审查工具定期对网络安全性进行检查和测试；如果发现网络存在安全漏洞，则需要修改、完善网络安全配置；另外，除主动进行的安全审查外，当发生的网络安全事件证明网络还存在安全漏洞时，则也要对网络安全配置进行修改、完善。

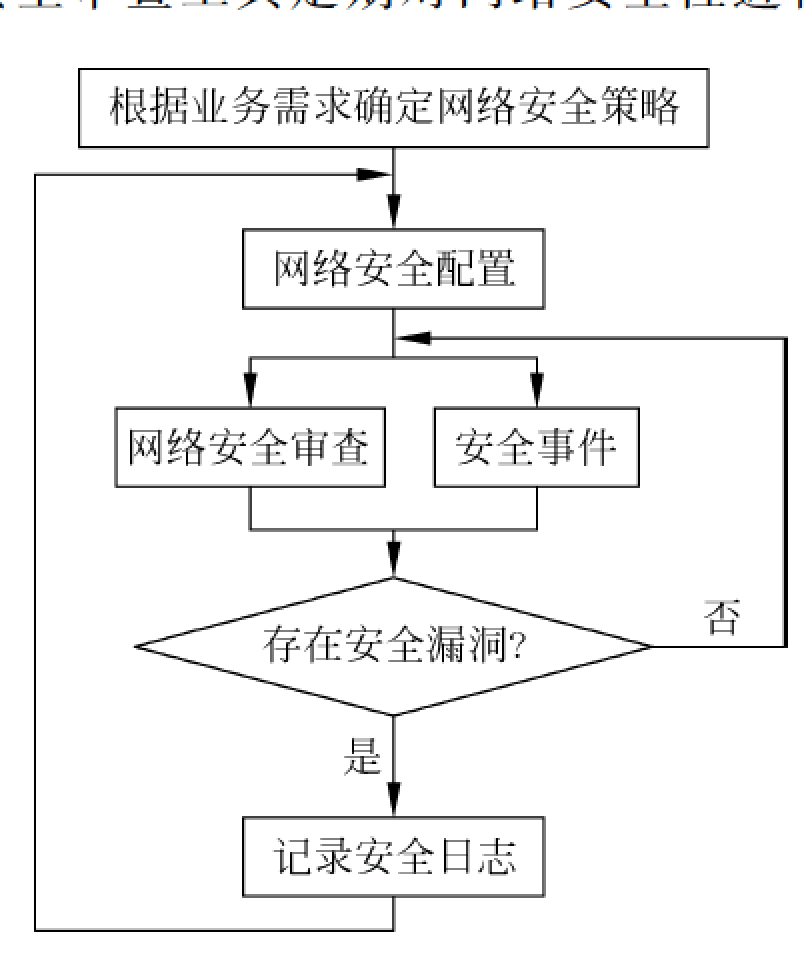


图 7-7　网络管理管理工作流程

3. 网络安全管理技术

目前常用的网络安全管理技术如下。

- 加密技术。
- 认证技术。
- 防火墙、访问过滤技术。
- VPN 技术。
- 入侵检测与防御技术。
- 防病毒技术。

- 备份与恢复技术。
- 安全风险扫描技术。

4. 网络安全管理需遵循的标准与制度

在进行网络管理时，需参照国家、国际有关标准进行。我国已经在网络安全方面制定了一些标准，如对网络系统安全级别进行定义的 GB 17859—1999《计算机信息系统安全保护等级划分准则》，对信息安全技术安全性进行定义的 GB/T 18336—2001《信息技术 安全技术 信息技术安全性评估准则》，对网络物理安全进行定义的 GB 9361—1988《计算机站场地安全要求》、GB 2887—2000《电子计算机场地通用规范》、GB 50174—1993《电子计算机机房设计规范》等，同时还有各类网络设备，如交换机、路由器安全技术要求相关标准，对各种网络，如软交换网络、公众 IP 网络的安全要求标准等。

7.5.2 网络安全审查

网络安全审查是指根据网络安全需求和网络安全标准对网络进行网络安全风险检查、评估的过程。目前有很多专门的网络安全漏洞扫描软件，如 Nessus、SAINT 等，可以对各种操作系统、网络设备进行安全漏洞扫描。

Nessus 软件可以扫描网络上的主机、网络设备，并将其与所存的安全漏洞定义库进行比较，检查其是否在访问控制、系统 bug 等方面存在安全漏洞。如图 7-8 所示为使用 Nessus 对某系统进行扫描后的结果。

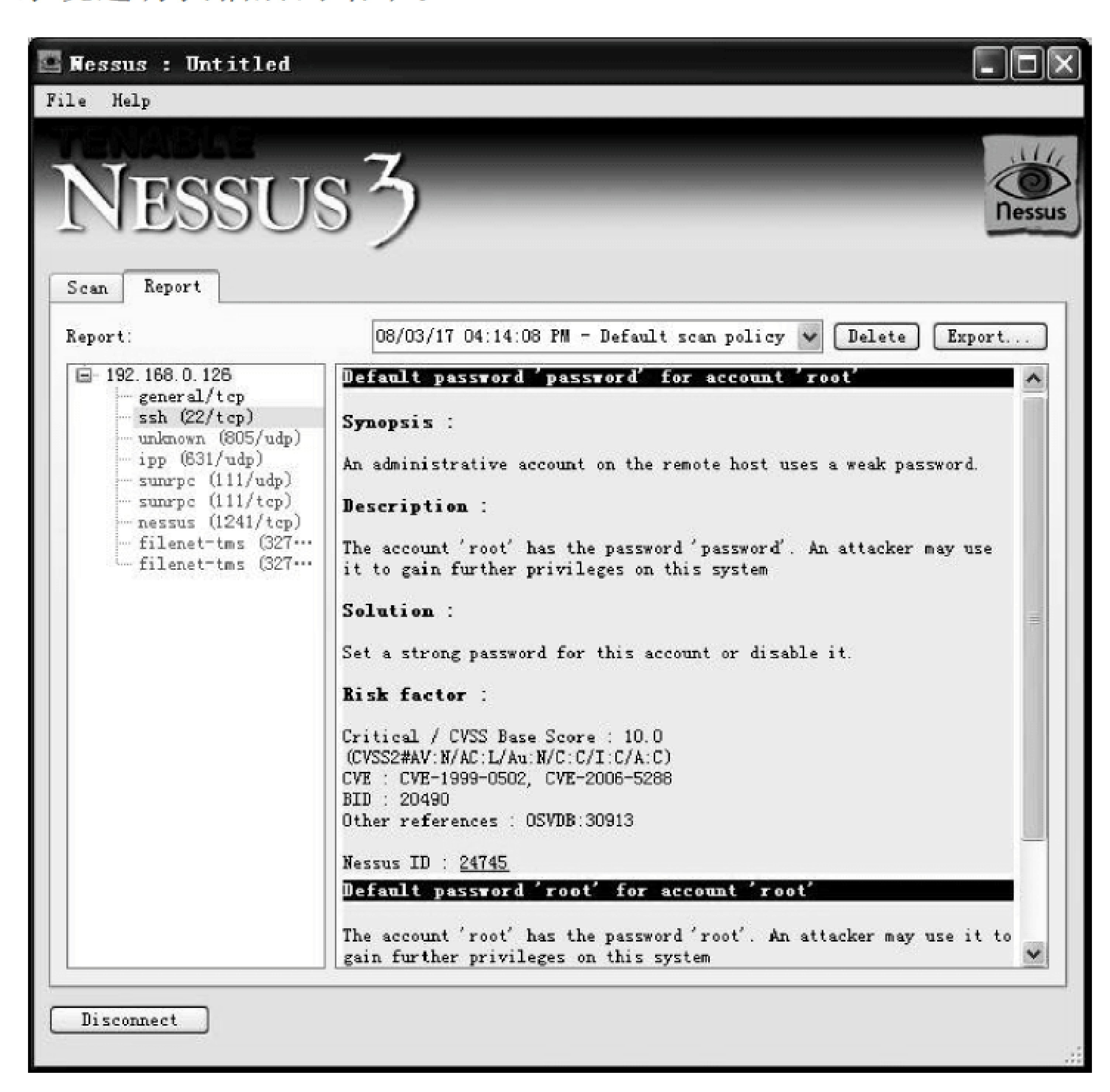


图 7-8 Nessus 安全扫描结果

Nessus 检查结果中会给出安全漏洞对应的风险标识号，检索 CVE、BID、OSVDB 等安全漏洞网站，可以查看到该风险标识号对应的解决建议。CVE、BID、OSVDB 等就像字典表，会为广泛认同的信息安全漏洞、已经暴露出来的弱点、已经发现的蠕虫等给出一个公共的名称。

7.5.3　入侵检测与入侵防御

1. 入侵检测与入侵防御简介

入侵检测是一种用于发现网络入侵行为的技术，提供入侵检测功能的系统称为入侵检测系统（IDS）。入侵检测系统通过检查所收集网络数据报文是否具有入侵特征，或网络是否出现异常，来判断是否网络是否受到入侵。入侵检测系统一般以旁路方式接入在高安全等级网络入口处，如图 7-9 所示。

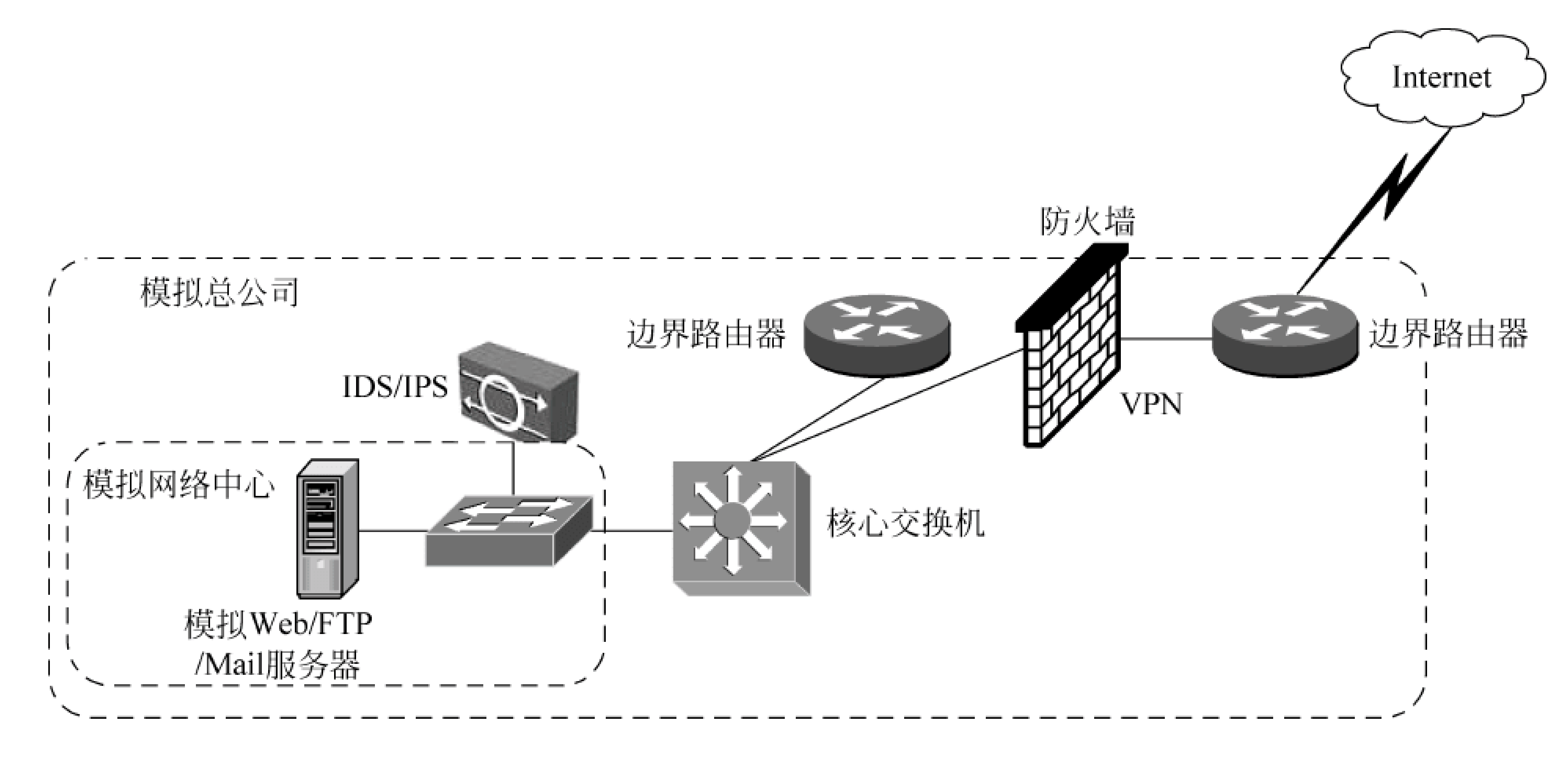


图 7-9　IDS/IPS 接入示例

入侵防御（IPS）技术是能够发现网络入侵行为，并进行自防御的技术。相对 IDS，入侵防御在发现入侵后，会发出警报、丢弃数据包和重置连接。

2. 入侵检测配置

在 Cisco PIX 防火墙上配置入侵检测/防御的步骤如表 7-3 所示。

表 7-3　Cisco PIX 防火墙入侵检测配置步骤

序　号	操　　作	相 关 命 令	必要性
步骤 1	创建审计策略	**ip audit…info**	是
步骤 2	定义入侵检测行为	**ip audit…attack**	是
步骤 3	在接口上应用审计策略	**ip audit interface**	是
步骤 4	检查入侵检测统计信息	**show ip audit count**	可选
步骤 5	动态阻挡网络连接	**shun**	可选

（1）创建审计策略，定义默认防御行为

在 Cisco PIX 防火墙上，创建审计策略并指定审计信息特征码默认行为的操作为在全局配置模式下输入：

ip audit name 审计策略名 info [action[alarm][drop][reset]]

参数 audit name 为审计策略名。

参数 info 表示为信息类特征码定义执行的动作。表 7-4 显示了 Cisco PIX 防火墙上的一些消息特征码，当防火墙发现存在以下特征的网络流量时，将按照审计策略定义执行相应的动作。

表 7-4 Cisco PIX 防火墙上的消息特征码

消息号	特征码 ID	特征码名	特征码类型	消息号	特征码 ID	特征码名	特征码类型
400000	1000	IP 选项-坏选项列表	信息	400014	2004	ICMP 回声请求	信息
400001	1001	IP 选项-记录数据包路由	信息	400023	2150	分段的 ICMP 流	攻击
400002	1002	IP 选项-时间戳	信息	400024	2151	大量 ICMP 流	攻击
400003	1003	IP 选项-安全	信息	400025	2154	死亡之 ping 攻击	攻击
400007	1100	IP 分段攻击	攻击	400032	4051	UDP snork 攻击	攻击
400010	2000	ICMP 回声响应	信息	400035	6051	DNS 区跳转	攻击
400011	2001	ICMP 主机不可达	信息	400041	6103	被代理的 RPC 请求	攻击
400013	2003	ICMP 重定向					

参数 alarm 表示发送警告。

参数 drop 表示丢弃数据。

参数 reset 表示丢弃数据包，同时还会关闭该数据包属于的连接。

(2) 定义入侵防御行为

在 Cisco PIX 防火墙上，入侵检测行为策略的操作为在全局配置模式下输入：

ip audit name 审计策略名 attack [action [alarm] [drop] [reset]]

(3) 在接口上应用审计策略

在 Cisco PIX 防火墙上，应用审计策略的操作为在全局配置模式下输入：

ip audit interface 接口名 审计策略名

(4) 检查入侵检测统计信息

在 Cisco PIX 防火墙上，检查入侵检测统计信息的操作为在特权模式下输入：

show ip audit count

(5) 动态阻挡网络连接

在 Cisco PIX 防火墙上，动态阻挡网络连接的操作为在全局模式下输入：

shun 被阻挡的源 IP [被阻挡的目的 IP 源端口 目的端口 [协议]]

该命令将配置动态阻挡，阻挡从某个 IP 地址端口到某个 IP 地址端口的连接。

例如，如果希望对于匹配攻击特征码后的数据执行警告和重置连接动作，对于匹配信息特征码后的报文执行警告动作的命令如下。

```
zb-fw0(config)# ip audit name attids attack action alarm reset
zb-fw0(config)# ip audit name inforids info action alarm
zb-fw0(config)# ip audit interface outside attids
zb-fw0(config)# ip audit interface dmz inforids
zb-fw0(config)# ip audit interface inside inforids
zb-fw0(config)# shun 10.0.0.10
Shun 10.0.0.10 addedincontext:single_vf
Shun 10.0.0.10 successful
```

7.5.4 防病毒技术

随着网络的普及和计算机病毒的发展,目前的计算机病毒侵害的对象不再只是单台主机,而是整个网络。所以网络安全管理,尤其是局域网网络安全管理中一项重要的工作是进行病毒防护的布控。

1. 常见病毒种类简介

目前常见的网络病毒种类如下。

(1) 系统病毒:感染特定的操作系统中的文件,例如 Windows 系统中的 *.exe 和 *.dll 文件,并通过这些文件进行传播。例如 CIH 病毒。防病毒软件通常使用 Win32、PE、Win95 等作为前缀定义该类病毒。

(2) 蠕虫病毒:通过网络或者系统漏洞在网络上进行传播,阻塞网络。例如冲击波病毒、小邮差病毒。防病毒软件通常使用 Worm 作为前缀定义该类病毒。

(3) 木马病毒:该类病毒的特点是通过网络或者系统漏洞进入用户系统并将自己隐藏起来,然后向外界泄露用户信息。防病毒软件通常使用 Trojan 作为前缀定义该类病毒。

(4) 黑客病毒:该类病毒也是通过网络或者系统漏洞进入用户系统并将自己隐藏起来,但黑客病毒不仅泄露用户信息,还使用户主机可被黑客远程控制。防病毒软件通常使用 Hack 作为前缀定义该类病毒。

(5) 脚本病毒:通过网页传播,以 VBS、JavaScript 等脚本语言编写。防病毒软件通常使用 Script 作为前缀定义该类病毒。

(6) 宏病毒:是一类特殊的脚本病毒,通过微软 Office 处理的文件进行传播。防病毒软件通常使用 Macro 作为前缀定义该类病毒。

(7) 后门病毒:与木马病毒相似,通过网络传播,一旦侵入用户系统,则在系统上打开系统后门(某些监听端口)。防病毒软件通常使用 Backdoor 作为前缀定义该类病毒。

2. 病毒防护技术简介

目前主要的防病毒技术主要有:基因码检测技术、虚拟机技术、代码分析技术、主动防御技术。

(1) 基因码检测技术

基因码检测也被称为特征码检测。目前几乎所有防病毒软件主要使用的还是此种技术。其原理是利用病毒数据库里的病毒特征数据,与被扫描文件进行对比,从而找出被病毒感染的文件。但使用这类防病毒技术能够有效查杀病毒的基础是病毒库能够及时得到更新,病毒库中能收录最新的病毒特征数据。

（2）虚拟机技术

虚拟机技术是指防病毒软件在进行查杀病毒时，模拟出一个小型虚拟运行环境，让程序在该虚拟运行环境中试执行，从而使病毒暴露其攻击特征。使用此种技术可以发现大部分变形病毒和大量未知病毒。

（3）代码分析技术

代码分析技术是指通过分析指令出现顺序或特定代码组合等病毒特征来判断文件是否感染病毒的技术。即通过扫描病毒特定的行为或多种行为组合来判断文件是否感染了病毒。

（4）主动防御技术

主动防御技术是指全程监视进程行为，发现“违规”行为，就通知用户或直接终止进程的技术。通过监控 Windows 系统的注册表键值、系统文件、网络访问等变动情况，发现是否受到病毒侵害。其缺点是需要用户太多干预。

3．病毒防控的部署

病毒防控的部署工作主要包括以下几个方面。

（1）提高系统主机的抵御病毒侵害能力

当主机存在安全漏洞时，容易成为病毒侵害的对象。因此加强主机系统本身安全，及时更新系统，为系统打补丁是提高主机抗病毒能力的基础。

（2）保证病毒防护措施及时有效

如前所述，由于特征码检测是目前最主要的病毒防护措施，所以必须保证病毒库能及时更新。但在网络中有较多主机的情况下，逐台主机维护病毒库是不可行的。因此在部署防病毒软件时，可选用防病毒软件的网络版本。这种版本的防病毒软件，在网络中设置一台病毒库服务器，可以主动向网络中主机“推送”病毒库。

（3）加强人员网络安全培训

大部分病毒的传播是由于用户缺乏必要的网络安全防护知识，所以加强用户网络安全培训，提高用户防病毒意识，是遏制病毒泛滥的有效手段之一。

7.5.5 记录安全日志

通过安全日志，网络管理员可以获得网络安全事件的许多信息，但记录安全日志会消耗网络设备的网络资源，因此需在网络性能许可下谨慎配置。要记录网络节点的日志，需先安装配置 syslog 服务器，然后在网络节点上启用日志记录功能。

1．配置网络设备记录日志

在 Cisco 网络设备上配置进行日志记录的基本步骤如表 7-5 所示。表 7-6 列出了日志级别参数值。

表 7-5 启用网络设备安全日志功能的基本步骤

序 号	操 作	相关命令	必要性
步骤 1	启用日志记录功能	**logging enable** 或 **logging on**	是
步骤 2	指定 syslog 服务地址或主机名	**logging host**	是
步骤 3	指定日志级别	**logging trap**	是

表 7-6　日志级别参数值

级别值	日 志 级 别	含　　义
0	emergencies	系统不可用
1	alerts	报警，在端口上需要立即操作
2	critical	网络设备上存在一个关键状态
3	errors	网络设备上存在一个错误状态
4	warnings	网络设备上存在一个警告状态
5	notifications	网络设备上发生了一个重要的事件
6	informational	网络设备上发生了一个信息事件
7	debugging	来自 debug 命令的输出

例如，要将边界路由器日志写入到 200.100.8.25 上的配置操作如下。

```
zb-r0(config)# logging  on
zb-r0(config)# logging  host  200.100.8.25
zb-r0(config)# logging  trap  informational
```

2. 安装配置日志服务器

Kiwi Syslog Daemon 是一种常用的 Syslog 服务器。Kiwi Syslog Daemon 安装完成后，还需配置服务监听的地址和端口。运行 Kiwi Syslog Daemon，单击软件快捷菜单上的图标，打开如图 7-10 所示的配置窗口，配置服务监听的地址和端口。

在 Bind to address 文本框中输入 Syslog 服务器使用的地址。

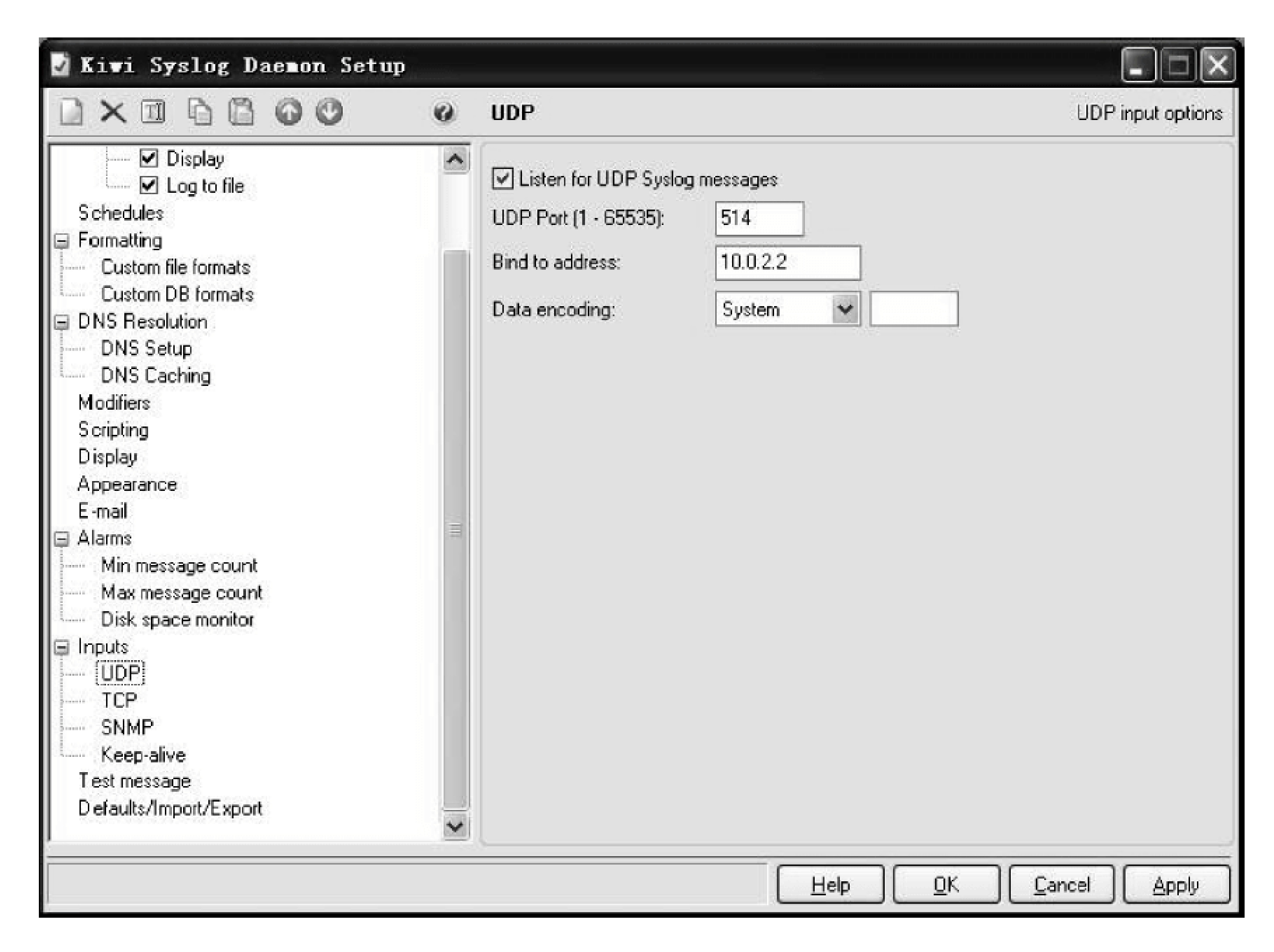


图 7-10　配置 Syslog 服务器监听地址和端口

当服务器在正确的地址和端口上开始监听日志记录请求时，网络设备上会出现如下提示信息，表示目前设备正在连接 Syslog 服务器，一旦连接成功，会在 Syslog 服务器主窗口中看到网络设备发来 log 信息。

```
*Sep  5 19:13:02.423: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 200.100.8.
25 started-CLI initiated
*Sep  5 19:13:02.423: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 200.100.8.
25 started-CLI initiated
```

7.6 网络性能管理

7.6.1 网络性能管理概述

计算机网络由网络设备、线路、网络服务等构成，网络性能管理需要对这些网络组件的运行状态、效率进行监控和调整，使网络能在满足通信需求的情况下更高效地工作。

1. 网络性能管理流程

网络性能管理的工作流程如图 7-11 所示。其中采集、分析网络性能数据，也被称为网络性能监控。

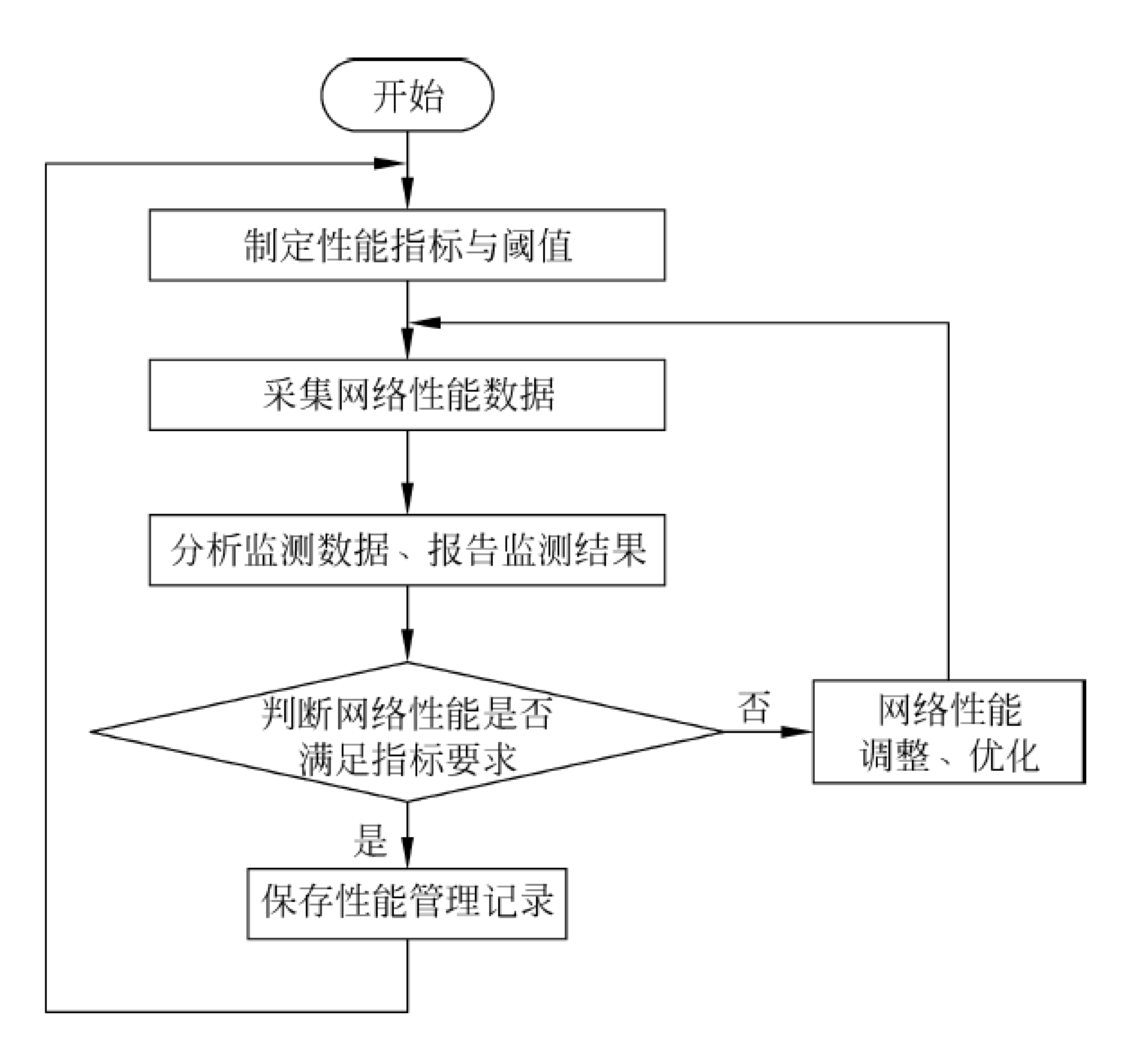


图 7-11 网络性能管理工作流程

2. 网络性能指标

评价网络性能通过评价网络是否满足某些性能指标来进行。常用网络性能指标包括如下几种。

(1) 网络总体性能指标：网络连通性、网络吞吐量、网络资源利用率、响应时间等。

(2) 网络节点性能指标：吞吐量、转发率、丢包率、节点处理时延等。

(3) 链路性能指标：带宽、信道利用率、带宽利用率等。

(4) 网络服务的性能指标：服务响应时间、最大并发连接数等。

3. 采集网络性能数据的方法

采集网络性能数据可从以下几个方面进行。

(1) 利用驻留在网络节点上的网络管理代理程序，采集网络性能数据。例如，通过配置网络设备上的 SNMP 代理，可以读取网络设备上 MIB 中有关网络性能的信息。表 7-7 显示了 Cisco Catalyst 2960 交换机 MIB 中与网络性能有关的部分对象。

表 7-7　Cisco Catalyst 2960 交换机 MIB 中的部分对象

对　象　名	功　　能	对　象　名	功　　能
ifSpeed	接口速率	ifOutQlen	接口出站队列长度
ifInOctets	接口入站流量速率	ifOutErrors	接口出站错误报文数
ifOutOctets	接口出站流量速率	ifInErrors	接口入站错误报文数

(2) 观察网络现有流量。例如，可通过网络监听工具(Wireshark、Sniffer 等)，捕获网络上现有数据包，分析数据报文是否存在广播风暴、是否有大量重传的数据包等，从侧面了解网络当前性能状况。

(3) 制造测试流量，并观察网络处理测试流量的情况。例如，可通过观察到某网络节点的 ping 包响应返回时间延迟，来获得两个网络节点间的网络时延信息。

7.6.2　利用网络节点上的网管代理监测网络性能

目前常用的网络设备或主机操作系统都支持 SNMP 网络管理功能。通过配置网络设备和主机上的 SNMP 代理程序，可使网管工具能够利用 SNMP 协议从网络设备或主机上直接采集网络性能数据，监控网络性能。

1. 网络设备 SNMP 代理配置

在 Cisco IOS 路由器或交换机上配置 SNMP 代理的基本操作步骤如表 7-8 所示。代理要与网络管理实体建立 SNMP 通信连接，必须先明确与网络管理实体通信使用的 SNMP 共同体名称、管理实体的地址，然后通过启用管理代理通知，使之向管理实体报告网络管理信息。

表 7-8　网络设备 SNMP 代理基本配置步骤

序　号	操　　作	相 关 命 令	必要
步骤 1	定义 SNMP 共同体	**snmp-server community**	是
步骤 2	指定 SNMP 管理实体地址	**snmp-server host**	是
步骤 3	启用 SNMP 代理通知	**snmp-server enable traps**	是
步骤 4	检查 SNMP 代理配置	**show running-configure** **show snmp**	可选

(1) 定义 SNMP 共同体

在 Cisco IOS 路由器或交换机上，创建 SNMP 共同体的操作为在全局配置模式下

输入：

snmp-server community snmp 共同体名 ［snmp 访问权限］

参数“snmp 共同体名”用于定义新建共同体的名称，共同体名称为一串字符。

参数“snmp 访问权限”用于定义使用该共同体名称的网络管理实体和代理通信时具有的操作权限。可选值分别为 rw、ro。

还可以在全局配置模式下输入如下命令，限制哪些管理实体可以使用指定的 SNMP 共同体名访问该网络设备。

snmp-server community snmp 共同体名 ［ACL 名或 ACL 号］

（2）指定 SNMP 管理实体地址

在 Cisco IOS 路由器或交换机上，指定 SNMP 管理实体地址的操作为在全局配置模式下输入：

snmp-server host snmp 管理实体 IP 地址 snmp 共同体名

例如，如果基于 SNMP 的网络监控软件安装在主机 192.168.0.254 上，而 snmp 共同体名为 test，则可以在网络设备上输入如下命令创建相应 SNMP 共同体，并定义网络设备网络管理代理所对应的管理实体地址。

```
C2960-1-2-1(config)#snmp-server community test
C2960-1-2-1(config)#snmp-server host 192.168.1.2 test
```

（3）启用 SNMP 代理通知

在 Cisco IOS 路由器或交换机上，启用 SNMP 代理向网络管理实体发送通知的操作为在全局配置模式下输入：

snmp-server enable traps ［通知信息类型］

该命令可不带参数使用，此时会默认启用所有通知。

（4）检查 SNMP 代理配置

在 Cisco IOS 路由器或交换机上，可以使用 show snmp 命令检查网络设备上 SNMP 代理的配置信息。

例如，检查网络设备上配置的 SNMP 共同体信息，可在特权配置模式下输入：

show snmp community

该命令的输出结果如下。

```
C2960-1-2-1#show snmp community

Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only active
```

```
Community name: test
Community Index: cisco1
Community SecurityName: test
storage-type: nonvolatile    active
```

又如，要检查网络设备上配置的网络管理实体地址信息，可在特权模式下输入：

show　snmp　host

该命令的输出结果如下。

```
C2960-1-2-1#show snmp host
Notification host: 192.168.0.254    udp-port: 162   type: trap
user: test      security model: v1
```

通过 show snmp 命令还可以获得网络设备上 SNMP MIB 库的信息。例如，可以通过 show snmp mib 命令了解网络设备现有 MIB 中，可被管对象及其 OID 等信息。

show snmp mib 命令的输出结果如下。

```
C2960-1-2-1#show  snmp  mib
此处省略部分显示...
ifNumber
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
ifPhysAddress
ifAdminStatus
ifOperStatus
ifLastChange
ifInOctets
ifInUcastPkts
此处省略部分显示...
ip.1
此处省略部分显示...
icmp.1
此处省略部分显示...
```

2. 网络性能监控软件的安装配置

PRTG 是一款基于 Windows 平台的网络性能监控软件，它能够通过 SNMP 协议与网络节点上的网络管理代理通信，获取网络节点上的 MIB 信息，并通过图表方式显示出来。

（1）安装 PRTG

从 www.paessler.com/prtg/download 可以下载 PRTG 的免费试用版。其安装非常

简单，只需双击运行安装程序，然后配置几项参数，逐步单击 Next 按钮即可。PRTG 安装过程中需要配置的参数如图 7-12 所示。

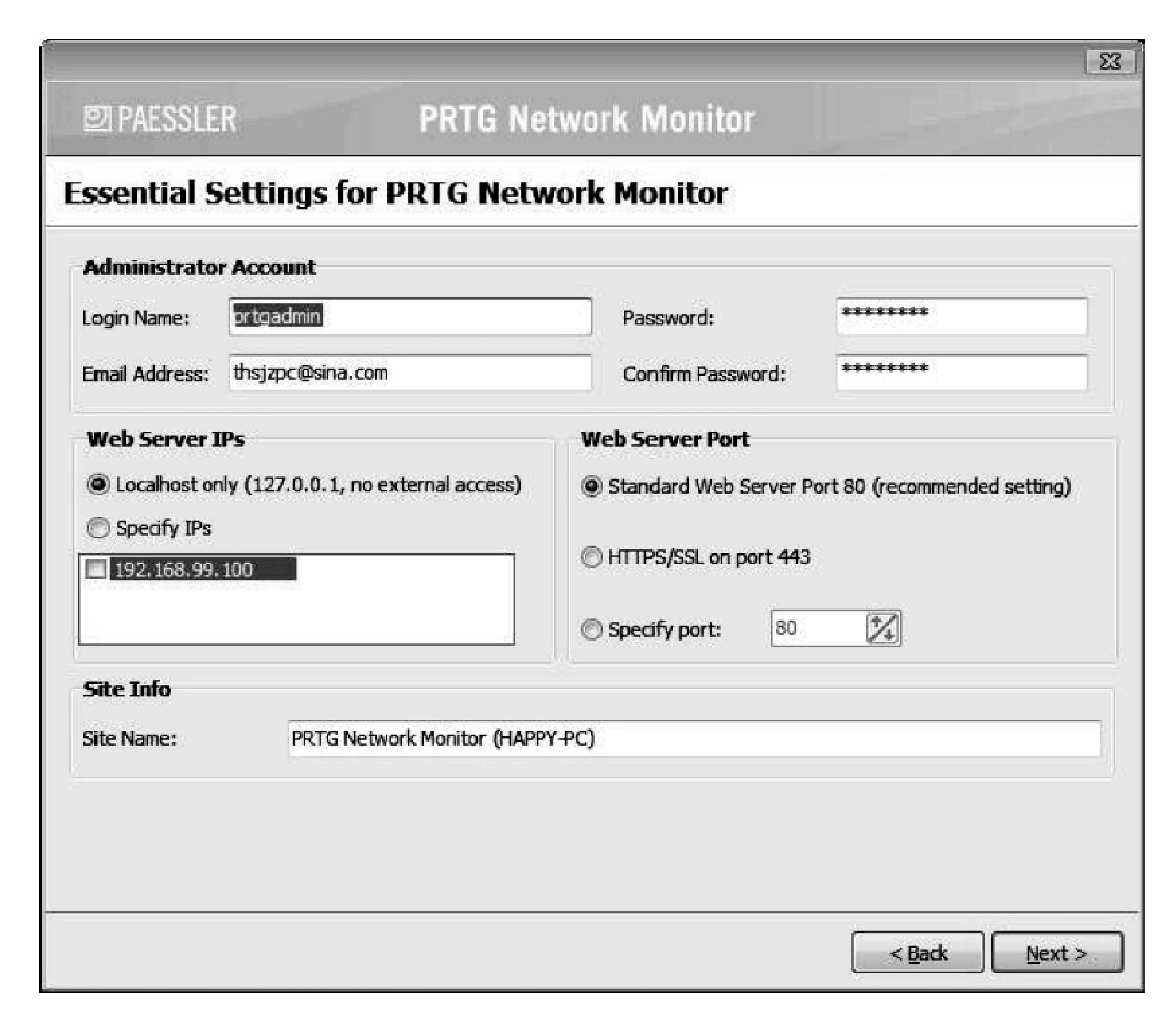


图 7-12 PRTG 监控服务器配置窗口

① PRTG 监测服务器工作的 IP 地址。由于最新支持 Web 页面显示功能的 PRTG，需要在 Windows 系统上创建一个 Web 服务器来显示 PRTG 获取的网络性能数据，所以在安装过程中，需输入该服务器工作的 IP 地址。

② 网络管理员邮件地址。PRTG 支持多种向网络管理员报告网络性能信息的方式，如电子邮件等，所以在安装过程中，还需输入网络管理员的电子邮件地址。

③ 登录 PRTG 的账号。PRTG 内嵌一个登录账号为 prtgadmin，口令为 prtgadmin。可以在安装过程中设置使用其他账号来登录 PRTG。

(2) 配置 PRTG 的监测网络性能

要在 PRTG 上监测网络性能，需完成以下配置步骤：在 PRTG 上创建被管设备条目、选择要监测的网络设备性能指标。

在 PRTG 上创建被管设备条目的操作如下。

双击 Windows 桌面上的 PRTG 图标，然后在图 7-13 所示窗口中输入账号 prtgadmin 和口令登录 PRTG。

登录 PRTG 后的主窗口如图 7-14 所示。单击窗口中的 Add Sensor(s) Manually 图标，为所要管理的设备创建新的感应器 Sensor。

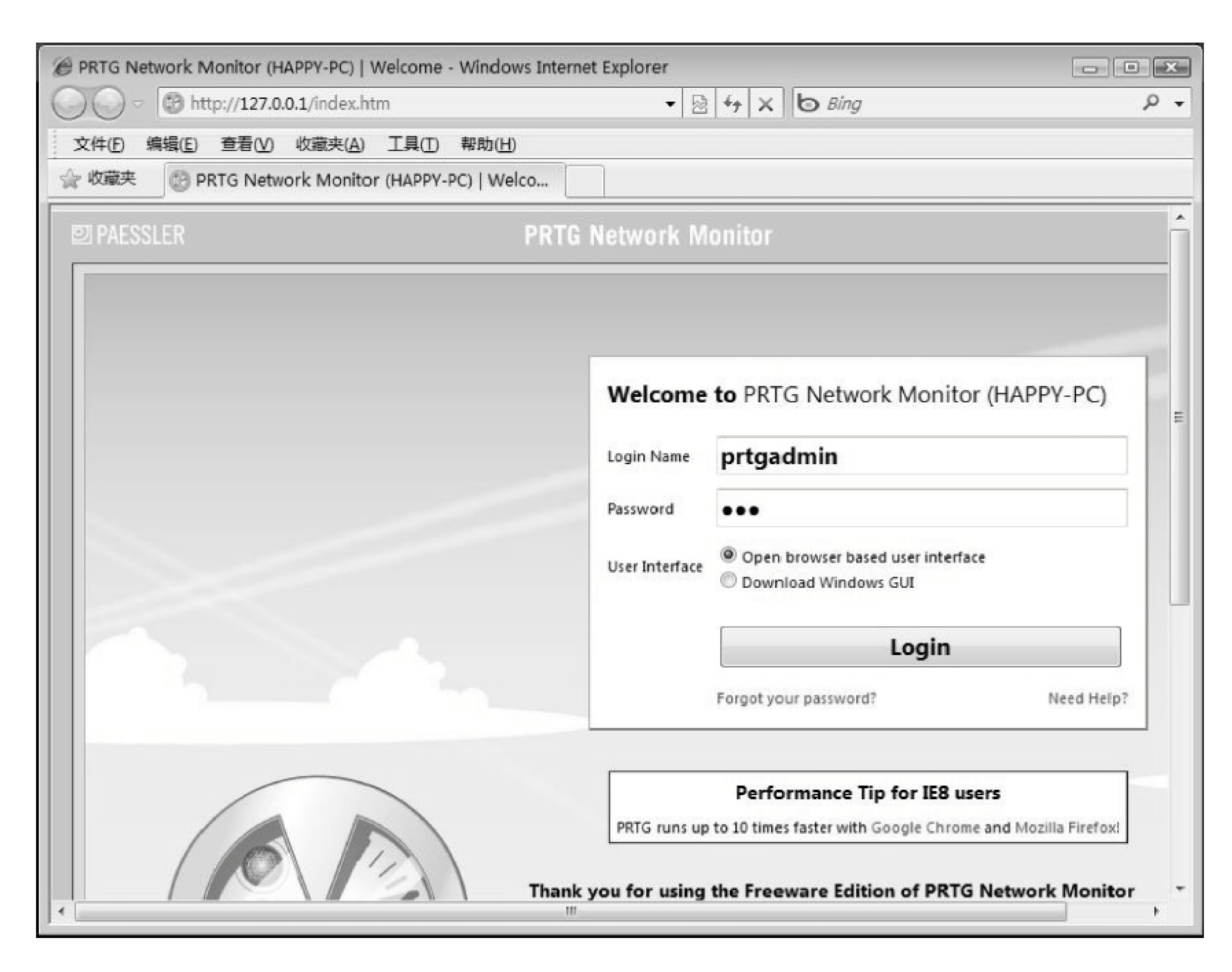


图 7-13　登录 PRTG 窗口

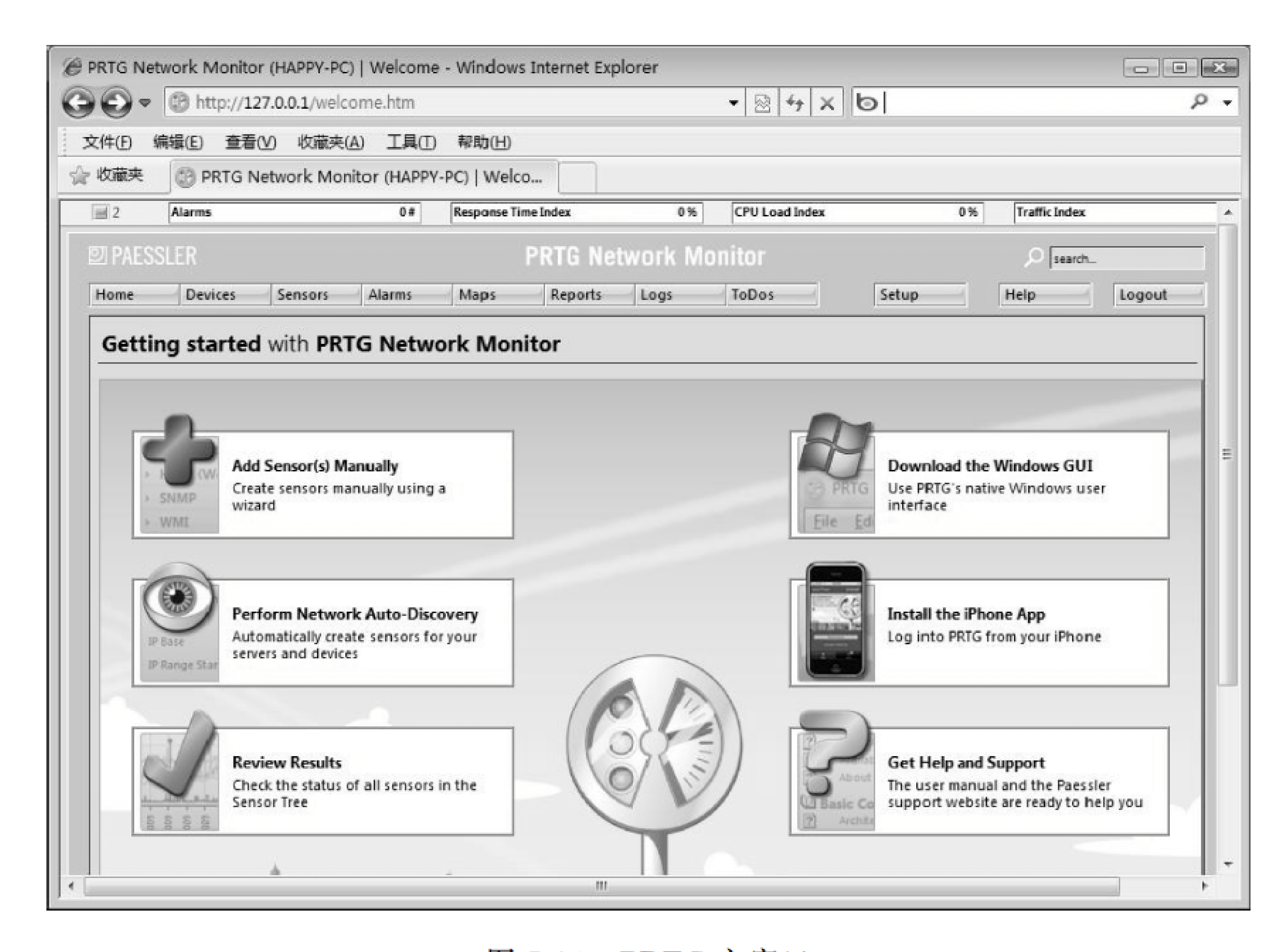


图 7-14　PRTG 主窗口

在接下来的图 7-15 所示的 PRTG 窗口中，先选中 Create a new Device 单选按钮，然后单击 Continue 按钮，为被管设备创建一个设备条目。



图 7-15 新创建设备窗口

由于 PRTG 将被管对象进行分组管理，所以还需在图 7-16 所示窗口中，选中 Create a new Group 单选按钮，然后单击 Continue 按钮，选择新建一个组。

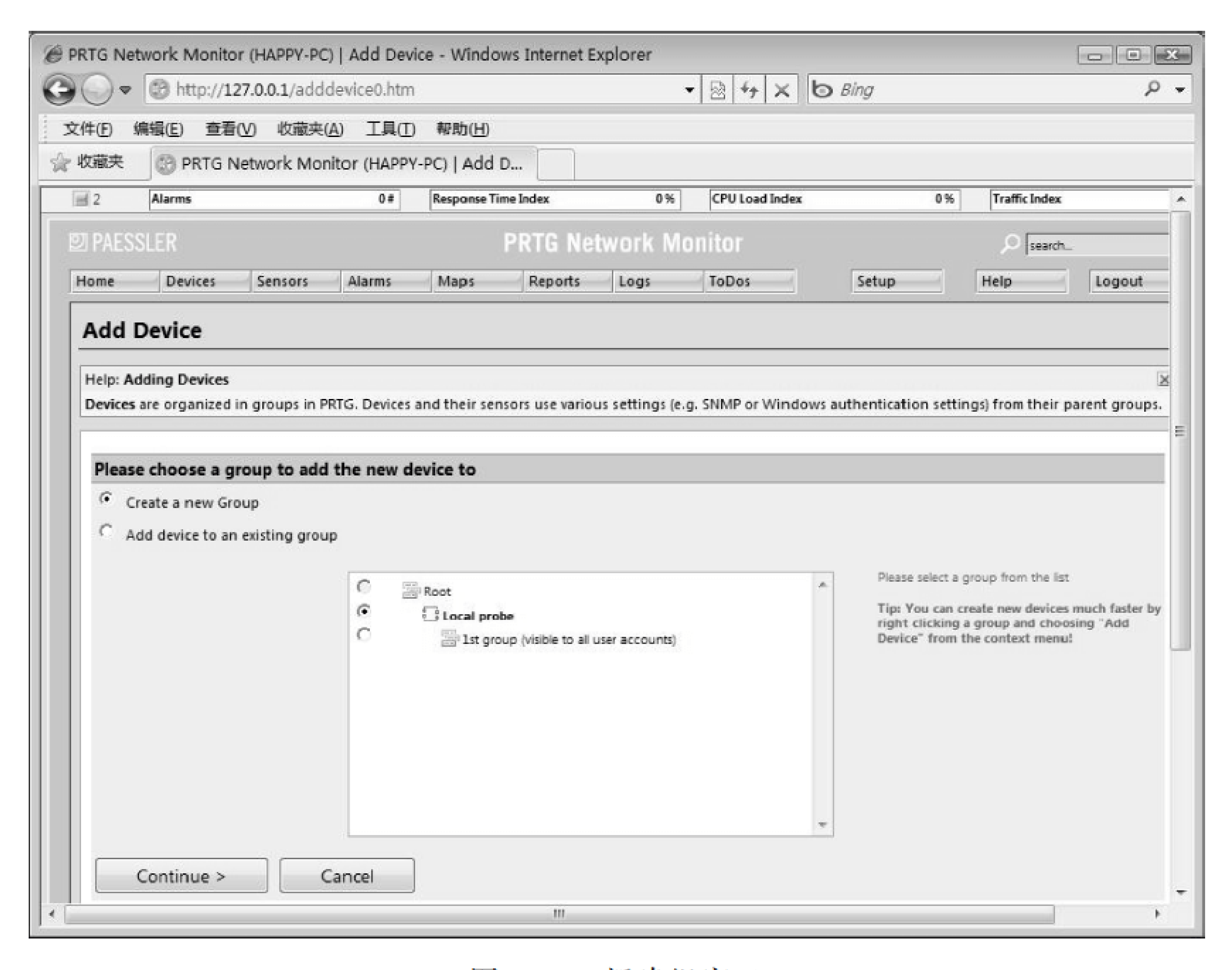


图 7-16 新建组窗口

PRTG 接下来显示图 7-17 所示的窗口，为组配置默认属性。例如，与管理代理程序通信使用的 SNMP 共同体名、SNMP 协议版本、通信端口等。

完成组的创建操作后，PRTG 会显示图 7-18 所示的组列表窗口，在其中选择新创建的组，单击该组下面的 Add Device 按钮，将进入图 7-19 所示的创建新设备条目窗口。

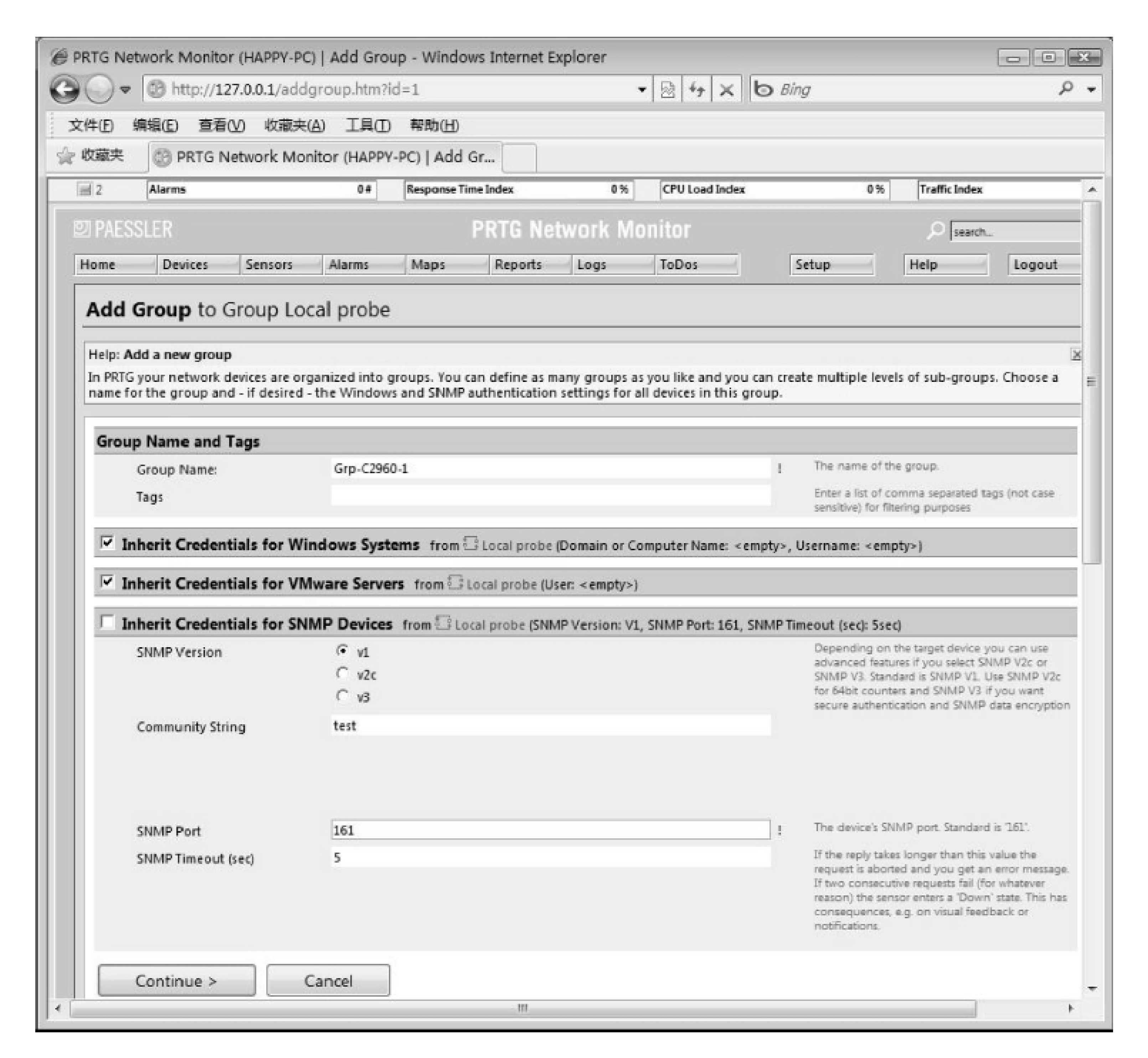


图 7-17　配置组的 SNMP 属性

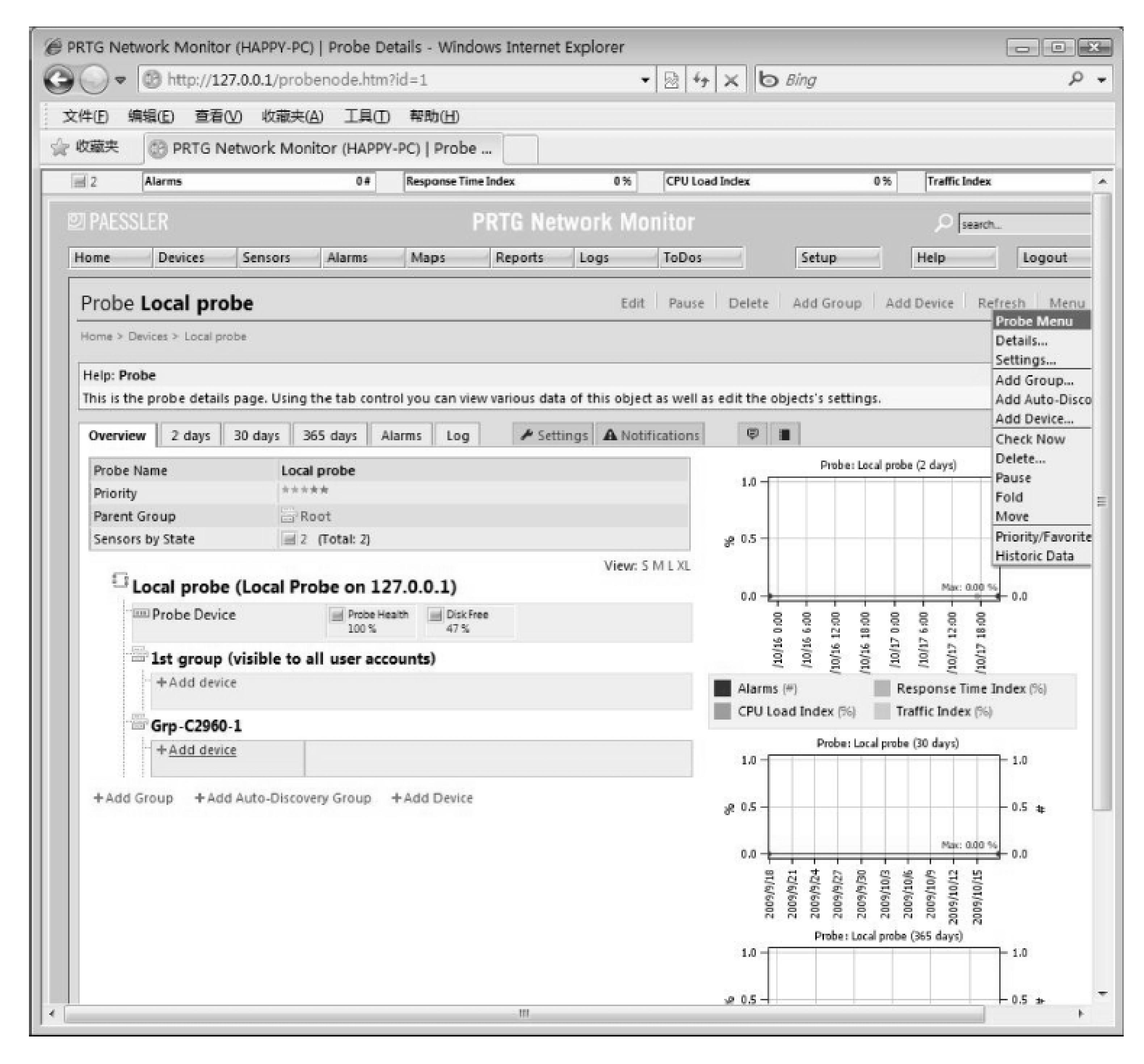


图 7-18　在组中添加新设备

在图 7-19 所示窗口中，必须配置的是 SNMP 通信属性。取消选中 Inherit Credentials for SNMP Devices 复选框，并在展开的窗口中，输入与管理代理程序通信使用的正确的 SNMP 共同体名，然后单击 Continue 按钮即可创建新设备条目。

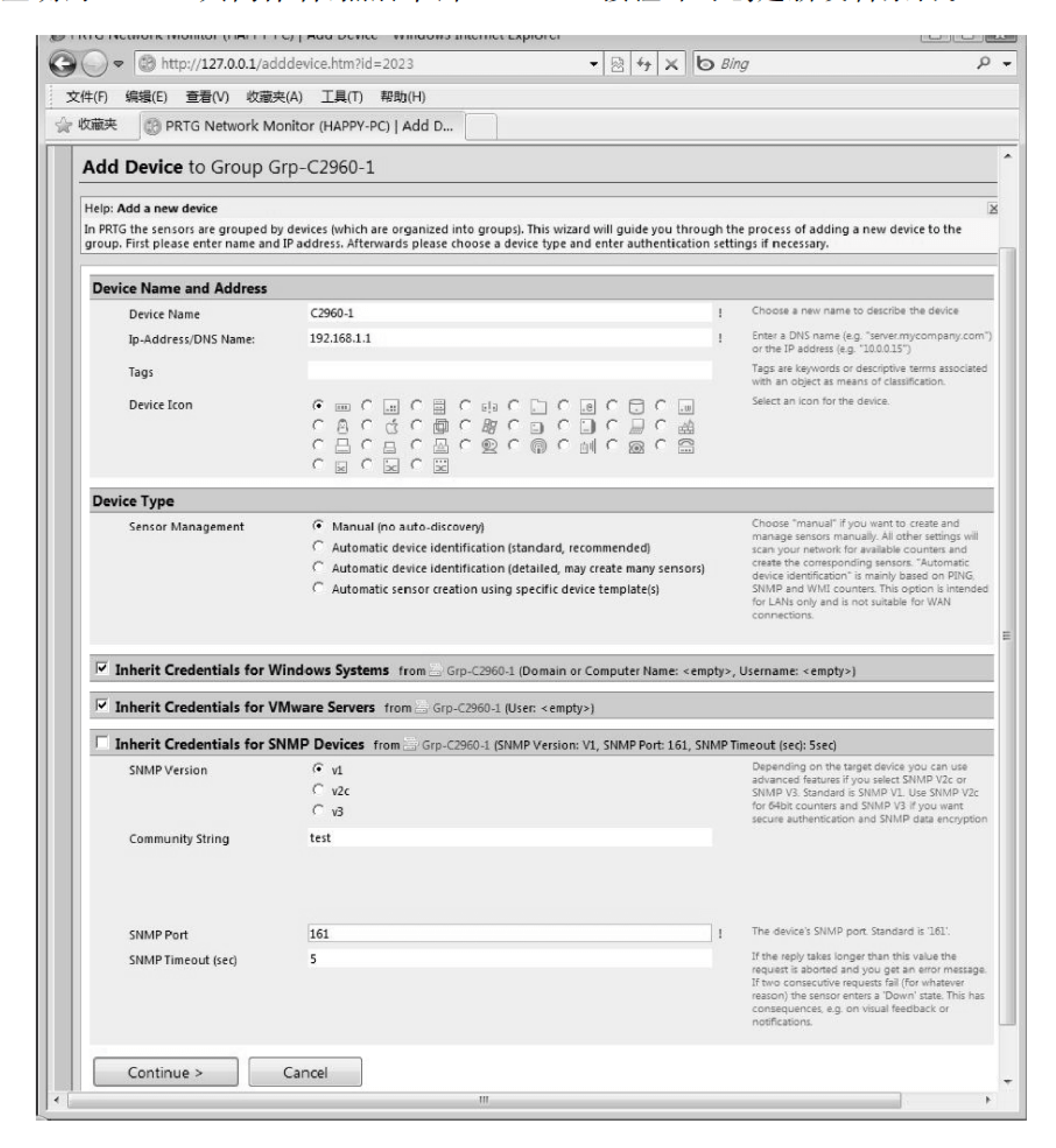


图 7-19　定义新设备相关属性

完成设备条目创建后，需要创建探测器 Sensor，才能监测网络设备上接口、链路的性能配置。在图 7-20 所示组列表窗口中，选择设备条目，单击其右侧的 Add Sensor 按钮可以为其创建 Sensor。

在创建 Sensor 窗口中，在 SNMP 选项卡中，选择创建使用 SNMP 协议获取信息的探测器。注意，由于 Cisco 网络设备使用其自己扩展的 MIB，所以要在 SNMP 探测器区域中选中 SNMP Library 单选按钮，选择探测器使用的 MIB，如图 7-21 所示。PRTG 附带了两个 Cisco MIB，一个是 Cisco Interface MIB，另一个是 Cisco Queue MIB。选择 Cisco 设备默认支持的 Cisco Interface MIB，单击 Continue to step 2 按钮，连接网络设备。

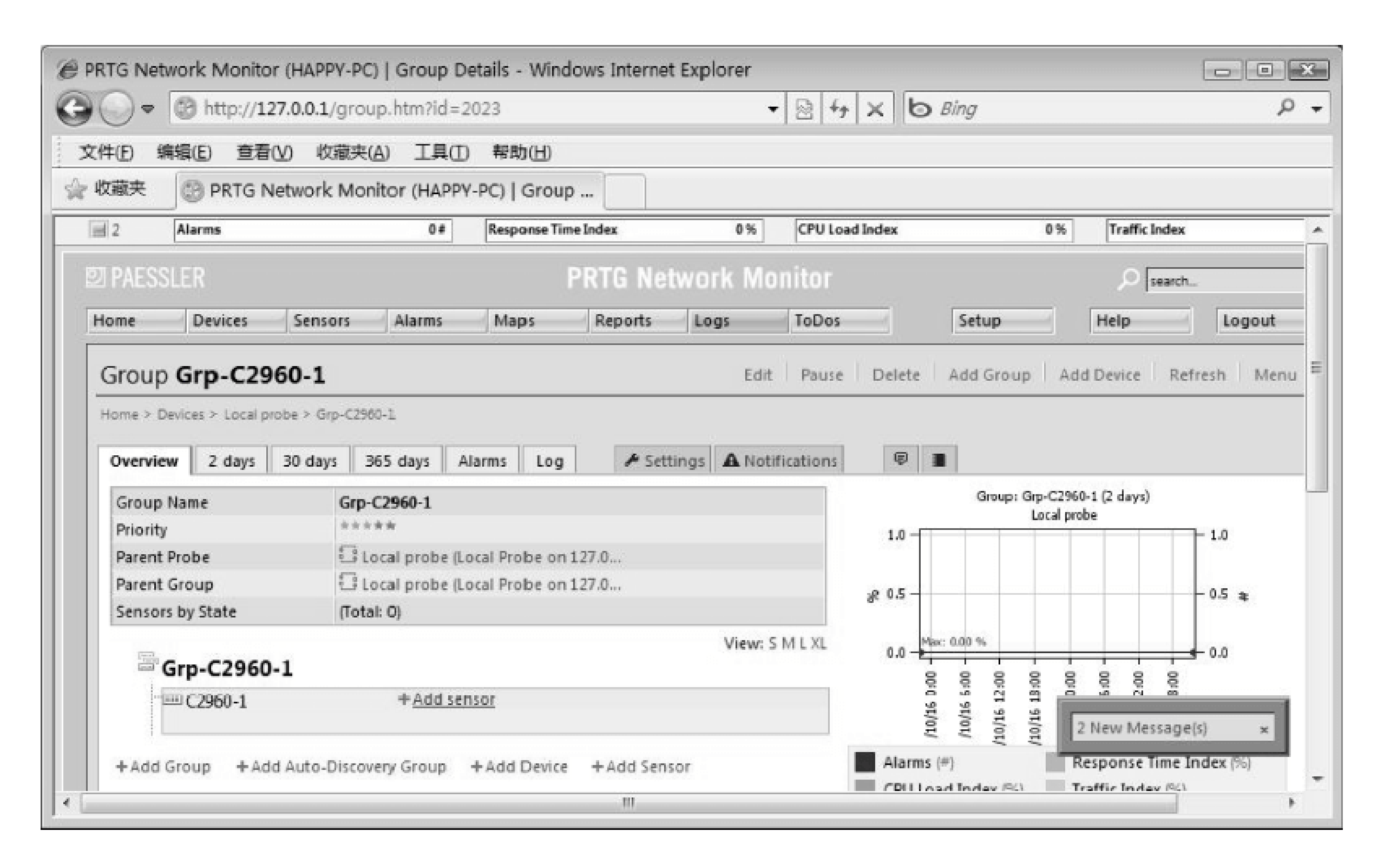


图 7-20　为新设备添加探测器

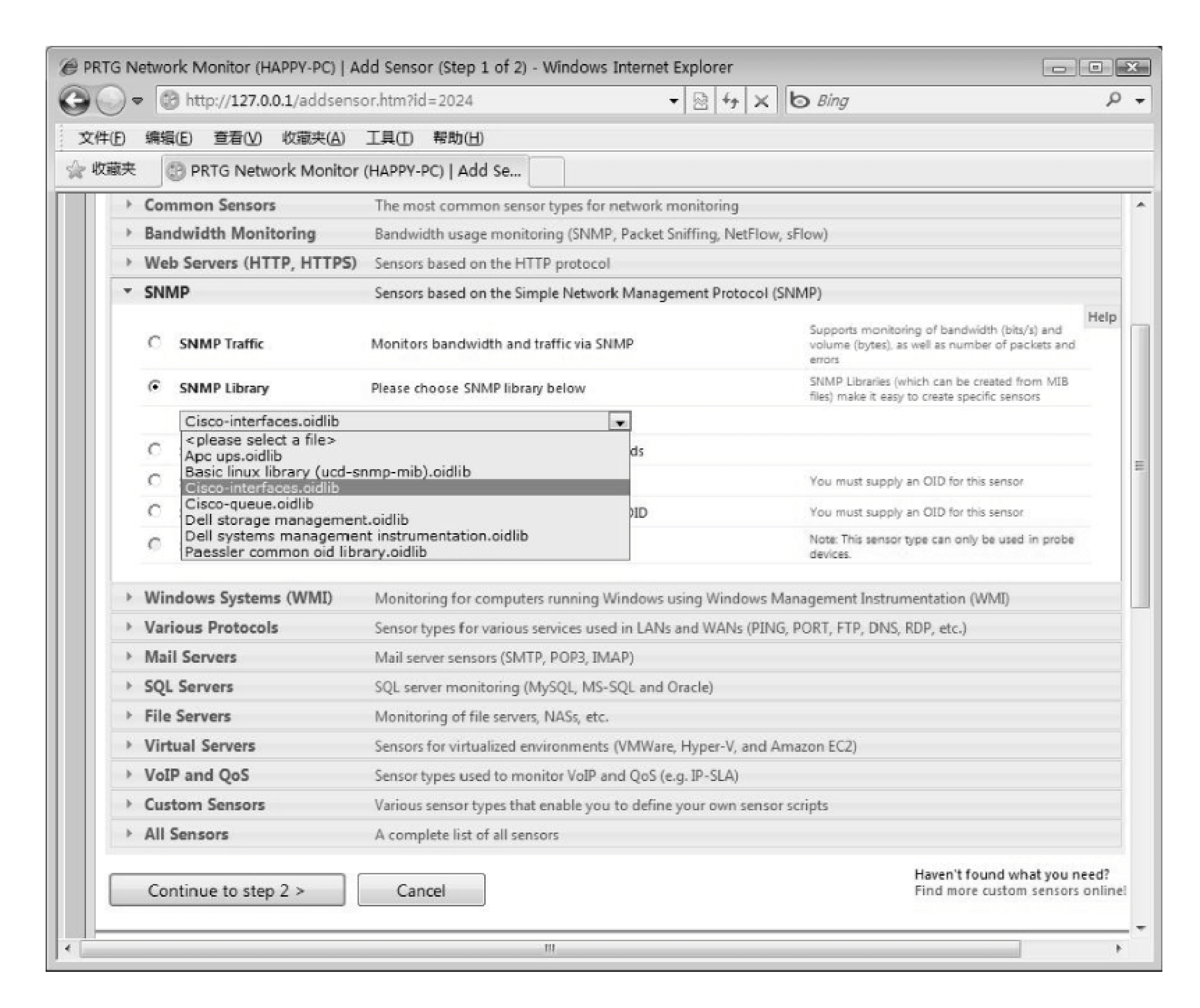


图 7-21　定义探测方式

在 PRTG 使用正确的 SNMP 共同体名连接到网络设备后，会显示图 7-22 所示的窗口，供管理员选择要探测的配置信息。该窗口中显示在网络设备 MIB 中的被管理对象信息条目，如 if index，即网络设备接口的索引号。在图 7-22 所示窗口中选择想要监测的网络设备信息条目，单击窗口下方的 Continue 按钮，则 PRTG 会根据所选生成相应的探测数据，显示在图 7-23 所示窗口中。一条被监测设备的信息条目被称为一个 Sensor。

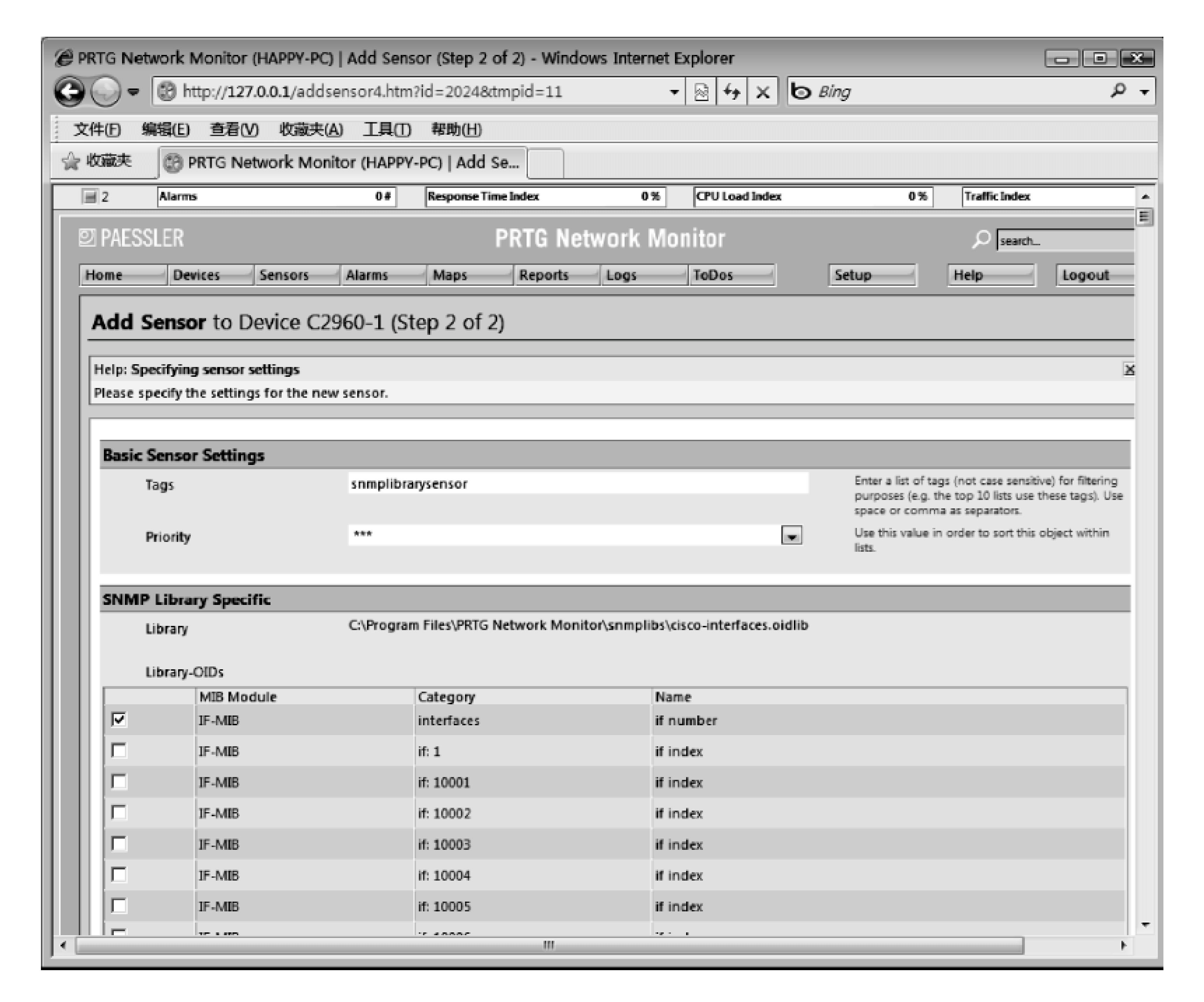


图 7-22 选择要探测的配置信息

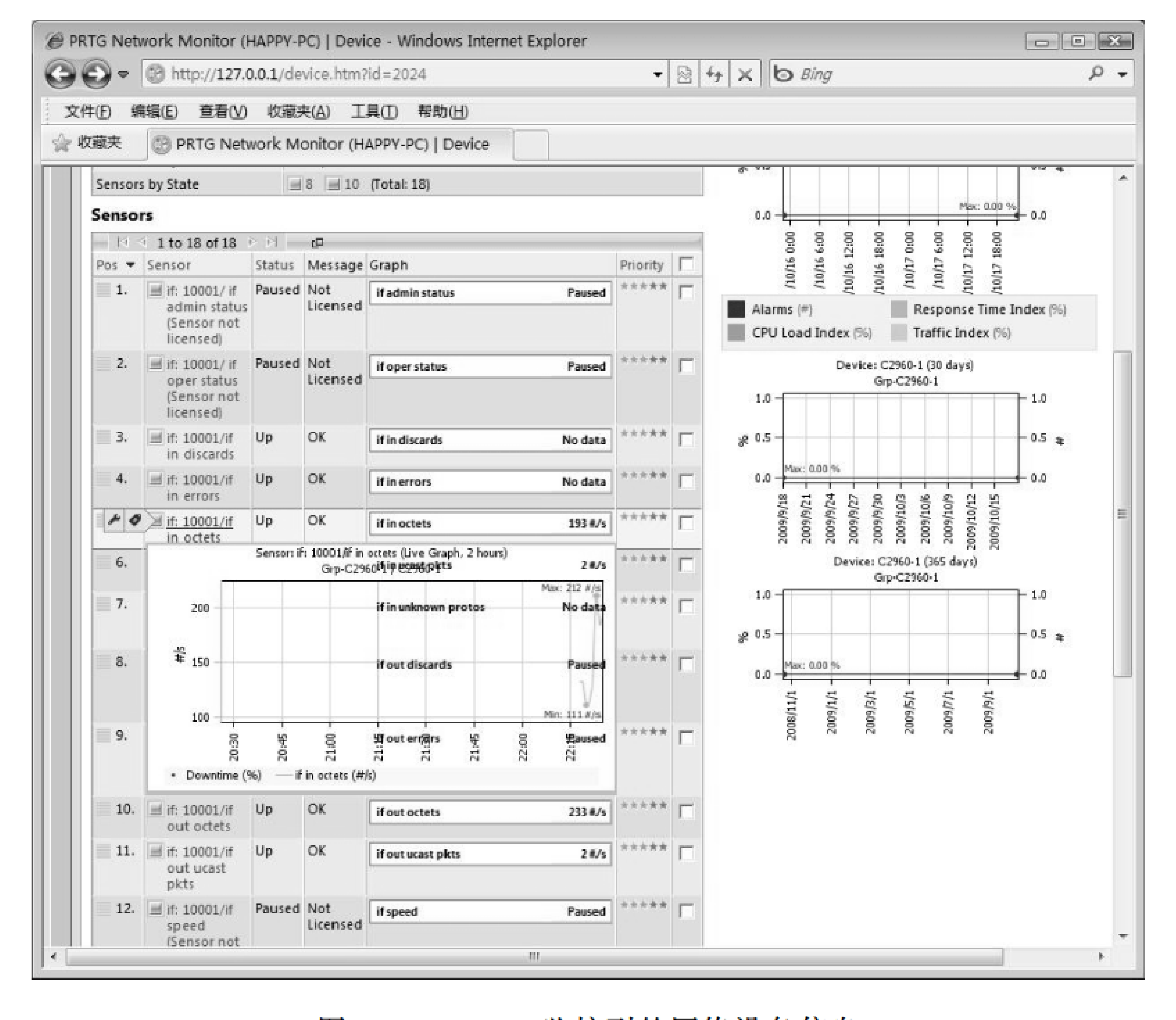


图 7-23 PRTG 监控到的网络设备信息

在图 7-23 所示窗口中，单击被监测的探测器，则会打开图 7-24 所示窗口，显示该探测器监测到的探测数据。通过这些探测数据，可以了解网络接口上的数据流量变化，并根据其应有的指标阈值，确定网络是否出现了拥塞、断路等情况。

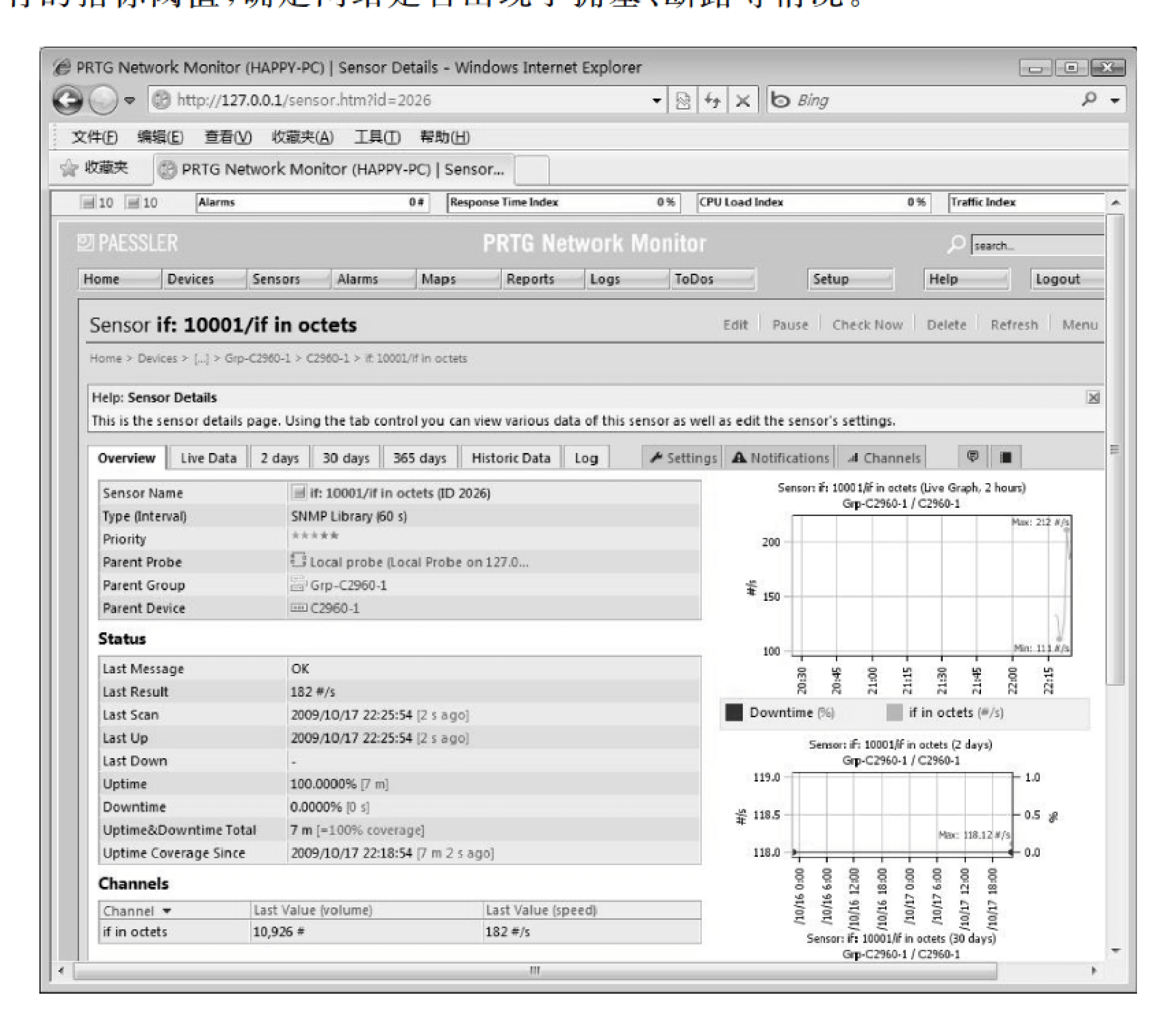


图 7-24　探测器详细信息

7.6.3　网络服务质量与网络性能保证

当网络性能不能满足网络需求时，可以根据具体情况来对网络进行优化、调整。而网络服务质量可以通过以下手段在一定程度上解决网络延迟、抖动和丢包等问题。

(1) 通过对数据报文进行标记和分类，使得网络设备可以区分不同优先级的通信流量，从而保证网络资源能更优先处理高优先级的通信流量。

(2) 通过调整使用的流量调节策略，可以为特定的通信需求提供更适合的通信流量控制方式。

(3) 可以将已经超过特定阈值的通信流标记为优先。

(4) 可以将超过特定速率阈值的通信流量丢弃，以避免拥塞。

1. 网络服务质量模型

IP 网络提供的是尽力传输的服务，目前在 IP 网络中使用的两种 QoS 体系模型是集成服务体系结构(Integrated Services Architecture，InServ)和区分服务体系结构(Differentiaed Services Architecture，DiffServ)。

(1) 集成服务体系结构。InServ 也称为硬 QoS，是一种严格预定的服务，使用资源预留协议(Resource Reservation Protocol，RSVP)实现。使用 InServ 则意味着所有中间系

统和资源都显式为通信流量提供预定的服务。

(2) 区分服务体系结构。DiffServ 也称为软 QoS，即不进行严格预定，而是以类别为基础对流量进行处理。某些类别的通信流量将优先于其他类别的通信流量得到处理。

2. 网络服务调度算法

在 IP 网络中，网络设备使用缓冲区和队列来处理通信数据，QoS 可以通过不同的队列管理、调度机制来调整通信流量被处理的方式。表 7-9 显示了常见的队列管理机制。

表 7-9 队列管理机制

排队机制	说明
先进先出 FIFO(First In First Out)	所有入站数据被加入到同一队列中，先进先出，所有数据包都是同一类别。这是 Cisco 网络设备默认的队列管理机制
加权循环 WRR(Weighted Round Robin)	数据包被配置不同的权重值，权重值越大，优先级越高，发生拥塞时，网络设备根据不同权重值分配不同的带宽比例
优先级排队	对于出站数据根据优先级进行调度，网络设备将优先处理严格优先级队列，然后才处理其他队列中的数据
整形循环 SSR 排队(Shaped Round Robin)	整形循环排队机制中，分为整形和共享两种模式。 整形模式下，网络设备对数据流量的处理类似于限速，出站流量均不能超过指定速率。共享模式下，网络设备按比例限制数据流的带宽，但在其他队列没有出站流量的情况下，单个队列可以占用整个带宽

3. QoS 的配置

在 Cisco Catalyst 交换机上配置 QoS 的步骤如表 7-10 所示。

表 7-10 Cisco Catalyst 交换机配置 QoS 的基本步骤

序号	操作	相关命令	必要性
步骤 1	启用 QoS	**mls qos**	是
步骤 2	创建类别映射表，定义哪些流量将被 QoS 处理 创建策略映射表	**class-map**、**ip access-list** 等 **policy-map**	是
步骤 3	定义交换机端口如何处理入站流量的 COS 值	**mls qos cos** **mls qos trust**	根据需要配置
步骤 4	定义 DSCP 映射	**mls qos map**	是
步骤 5	将策略映射表应用在端口的出入站流量上	**service-policy input|output**	是
步骤 6	定义端口上出站流量的拥塞管理机制	**wrr-queue**	是
步骤 7	检查 QoS 配置	**show class-map** **show mls qos aggregate-policer** **show mls qos maps** **show mls qos interface** **show policy-map**	可选

限于本书篇幅，有关路由器 QoS 配置相关命令细节参见 Cisco 技术手册。

7.7　模拟公司网络管理实现

受到网络管理成本限制，模拟公司没有购买大型网络管理平台，而是使用了随网络设备附带的网络管理工具和一些网络上免费的网络管理软件对网络进行管理。

（1）在配置管理方面，使用 Telnet、SSH 来实现配置的修改，使用免费网络拓扑发现工具来对网络拓扑进行管理。

（2）使用 PRTG 监控、记录网络性能变化，主要包括：广域网线路各条线路的流量、广域网线路的输入/输出情况、总流量以及丢包率、错包率，并在网络设备上配置 QoS 保证网络视频会议系统的运行。

（3）在总部边界防火墙上启用入侵检测，防御来自公网的入侵。

（4）定期对公司网络进行安全审查，扫描网络设备、节点等是否存在安全风险。

（5）公司各机构网络内设置有日志服务器，用于记录网络节点上的关键事件。

7.8　小结

网络管理包括故障、配置、记账、性能、安全 5 项内容。网络配置管理可通过 Telnet、SSH 进行，也可以通过专用网络管理软件，利用 SNMP 协议实现；网络故障管理分析定位可以使用分层、分段、替换、比较等方法进行；网络安全管理包括网络安全监测、网络安全审查和网络安全配置等方面；网络性能管理主要包括网络性能监测和网络性能调整两方面工作。网络管理软件可以通过驻留在网络设备上的网络管理代理获得网络设备性能状态。

7.9　习题

1. 简述网络故障排查定位的方法。
2. 简述采集网络性能指标的方法。
3. 简述网络性能管理中有哪些常用评价指标。
4. 简述什么是 MIB。
5. 简述 QoS 的 InServ 和 DiffServ 模型。

7.10　实训

1. 实训组织

实训学时：200 分钟。

学生分组：2 人/组。

2. 实训目的

（1）通过实训，熟练掌握为网络设备配置 Telnet 访问，并使用 Telnet 对设备进行远程管理配置的操作。

(2) 通过实训,熟练掌握故障排查定位方法。

(3) 通过实训,掌握在防火墙上配置网络入侵检测与防御的操作方法。

(4) 通过实训,掌握网络设备记录日志的配置方法,培养通过日志发现网络问题的能力。

(5) 通过实训,熟练掌握使用 PRTG 监控网络性能的方法。

3. 实训环境

(1) 安装有 Windows 系统、网络服务软件(例如 XAMPP)、网络攻击软件(例如 Smurf 等)、Syslog 服务软件的 PC,每组 3 台。

(2) Cisco PIX 防火墙,每组 1 台。

(3) Cisco 路由器,每组 1 台。

(4) UTP 交叉电缆,每组 4 条。

(5) Console 电缆,每组 1 条。

注意保持防火墙等网络设备为出厂配置。

4. 实训准备

按照图 7-25 所示连接网络设备,搭建实训环境。该网络拓扑为模拟公司网络简化而成,省略了部分与实训内容无关的网络设备。

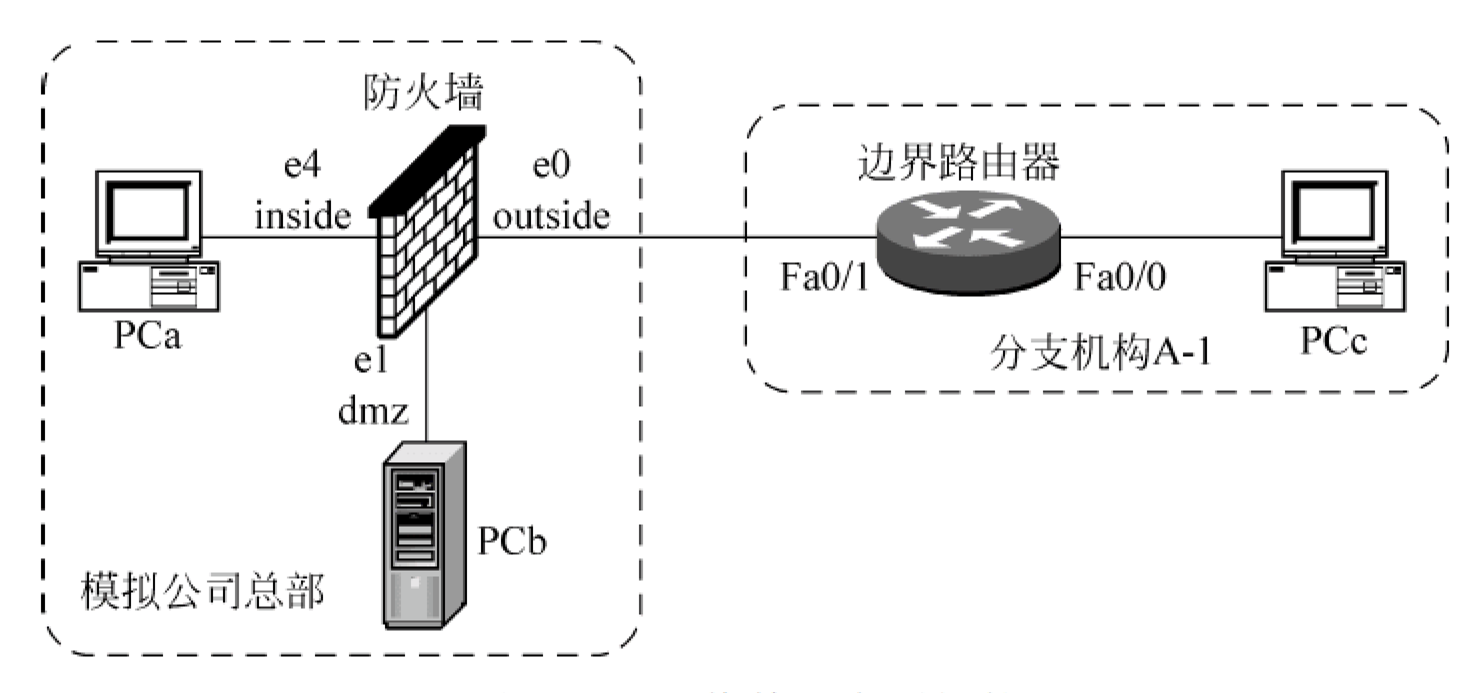


图 7-25 网络管理实训拓扑

该网络中 IP 地址分配如表 7-11 所示。其中 PCa 和 PCc 用于分别模拟各自网络中的日志服务器以及主机。在实训开始前,实验室教师需按表 7-11 配置好网络连接和路由。

表 7-11 网络管理实训地址分配

接 口	IP 地址/网络前缀	网 关
PCa(模拟内网主机、日志服务器)	200.100.8.122/30	200.100.8.121/30
PCb(模拟 FTP 服务器)	200.100.8.28/27	200.100.8.30/27
PCc(模拟外网主机、日志服务器)	200.100.15.198/30	200.100.8.121/30
防火墙 e0 接口(outside)	200.100.8.126/30	
防火墙 e1 接口(dmz)	200.100.8.30/27	
防火墙 e4 接口(inside)	200.100.8.121/30	
路由器 Fa0/0	200.100.8.125/30	
路由器 Fa0/1	200.100.15.197/30	

5. 实训内容

(1) 配置网络设备 Telnet 访问许可,并使用 Telnet 对设备进行远程管理。

(2) 网络入侵检测配置。

(3) 使用 PRTG 监控网络性能。

(4) 为网络设备记录日志。

(5) 故障排查定位。

6. 实训指导

(1) 配置网络设备 Telnet 访问许可,并使用 Telnet 对设备进行远程管理。在分支机构边界路由器和总部防火墙上分别配置 Telnet 访问许可,并使用 PCa、PCb、PCc 登录各网络设备,测试能否对网络设备进行配置。

在分支机构边界路由器上的参考配置操作如下。

```
a1(config)#enable secret 123
a1(config)#line vty 0 4
a1(config-line)#password 123
a1(config-line)#login
a1(config-line)#
```

在总部防火墙上的参考配置操作如下。

```
zbfw(config)# telnet 200.100.8.122 255.255.255.255 inside
zbfw(config)# passwd 123
zbfw(config)# enable password 123
```

(2) 为网络设备记录日志。启用分支机构边界路由器和总部防火墙上的日志记录功能,分别在 PCa、PCc 上启动 Syslog 服务器记录日志信息。

在分支机构边界路由器上,参考配置操作如下。

```
a1(config)# logging on
a1(config)# logging host 200.100.15.198
a1(config)# logging trap informational
```

在总部防火墙上,参考配置操作如下。

```
zbfw(config)# logging enable
zbfw(config)# logging host inside 200.100.8.122
zbfw(config)# logging trap informational
```

有关日志服务器配置参考本书 7.5.5 小节。

(3) 网络入侵检测配置。在总部防火墙上配置入侵检测与防御,并分别在 PCa、PCb、PCc 上运行攻击软件,攻击对方网络中的主机。检查防火墙的入侵检测与防御是否起到作用。

在总部防火墙上,配置入侵检测与防御参考配置操作如下。

```
zbfw(config)#ip audit name attids attack action alarm reset
zbfw(config)#ip audit name inforids info action alarm
```

```
zbfw(config)# ip audit interface outside attids
zbfw(config)# ip audit interface dmz inforids
zbfw(config)# ip audit interface inside inforids
```

有关网络攻击参考本书第 2、3 章部分内容。

(4) 使用 PRTG 监控网络性能。在分支机构边界路由器和总部防火墙上配置 SNMP 代理,在 PCb、PCc 上运行 PRTG 监控路由器和防火墙的接口流量变化。在 PCa 上通过浏览器从 PCb、PCc 上使用 FTP 下载大文件,观察网络设备接口流量信息的变化。

在分支机构边界路由器上,参考配置操作如下。

```
a1(config)# snmp-server community a1-pub
a1(config)# snmp-server host inside 200.100.15.198 a1-pub
a1(config)# snmp-server enable traps
```

在总部防火墙上,参考配置操作如下。

```
zbfw(config)# snmp-server community zb-pub
zbfw(config)# snmp-server host inside 200.100.8.122 zb-pub
zbfw(config)# snmp-server enable traps
```

有关 PRTG 配置参考本书 7.6.2 小节。

(5) 故障排查定位。通过网络攻击、物理破坏、错误配置等方式,分别设置网络服务、网络路由、网络链路、网络线路 4 种故障,提供给学生进行排查。

7. 实训报告

1. 根据实验指导配置。 能在 PCc 上使用 Telnet 远程登录到防火墙吗? 能□ 不能□ 为什么? ____________ 能在 PCb 上使用 Telnet 远程登录到防火墙吗? 能□ 不能□ 为什么? ____________
2. 在配置完日志记录后,分别在 PCa、PCb、PCc 上使用网络攻击软件发动攻击,记录在日志服务器上的相应记录。 PCa 攻击 PCb 时的日志记录: PCb 攻击 PCc 时的日志记录: PCc 攻击 PCa 时的日志记录:

续表

3. 在配置完日志记录和入侵检测后，分别在 PCa、PCb、PCc 上使用网络攻击软件发动攻击，记录在日志服务器上的相应记录。 PCa 攻击 PCb 时的日志记录：   PCb 攻击 PCc 时的日志记录：   PCc 攻击 PCa 时的日志记录：
4. 在路由器和防火墙上配置 SNMP 代理，并在 PCa、PCc 上配置 PRTG，监测并记录路由器和防火墙的接口流量信息。 路由器接口 Fa0/1 上的入站流量：平均值__________最大值__________ 防火墙接口 inside 上的入站流量：平均值__________最大值__________ 防火墙接口 outside 上的入站流量：平均值__________最大值__________ 防火墙接口 dmz 上的入站流量：平均值__________最大值__________
5. 在 PCb 上运行网络攻击软件，并在 PCa、PCc 上分别从对方服务器上使用 FTP 服务下载大文件，监测并记录路由器和防火墙的接口流量信息。 路由器接口 Fa0/1 上的入站流量：平均值__________最大值__________ 防火墙接口 inside 上的入站流量：平均值__________最大值__________ 防火墙接口 outside 上的入站流量：平均值__________最大值__________ 防火墙接口 dmz 上的入站流量：平均值__________最大值__________

附录 A

利用网络模拟器 GNS3 搭建模拟实训环境

由于使用真实网络设备进行实训成本较高,所以使用网络模拟器软件模拟网络设备进行网络实验就成为一种比较经济的替代方案。目前常见模拟 Cisco 网络设备的模拟器软件有思科网络学院的 PacketTracer、Routersim、Boson 实验模拟器和免费的 Dynamips、Pemu、GNS3 等。

GNS3(http://www.gns3.net)是一款图形化的网络模拟器,它集成了模拟路由器的 Dynamips 和模拟 Cisco PIX 防火墙的 Pemu 模拟器软件,可以使用图形化界面搭建网络模拟环境。Dynamips、Pemu 的优点是直接使用 Cisco 网络设备的 IOS 映像文件进行模拟,操作更真实。

GNS3 可以模拟路由器、防火墙,但对 PC 和交换机的模拟功能较差。

如果实训环境需要多台 PC,则可以安装虚拟 PC 模拟器来辅助 GNS3 解决问题。Virtual PC Simulator 软件是一款开源 PC 模拟软件,可以模拟 9 台虚拟 PC,并支持对这些 PC 配置 IP,运行 ping、traceroute 命令等。通过虚拟 PC 模拟器 Virtual PC Simulator 与 GNS3 的 cloud 图标结合,可以实现在 GNS3 中模拟多台虚拟 PC。

GNS3 中不支持交换机的模拟,但可以使用带交换模块的 3700、3600 系列路由器来模拟部分交换机功能。

A.1 安装并配置 GNS3 初始环境

A.1.1 安装 GNS3

安装 GNS3 的操作非常简单,首先从 GNS3 官方网站 http://www.gns3.net/download 下载 GNS3 模拟器软件,例如 GNS3-0.6.1-win32-all-in-one.exe;然后打开 Windows 资源管理器,找到下载的 GNS3 模拟器软件,双击进行安装。GNS3 需要 Winpcap 支持,所以安装过程中会提问是否安装该软件,按照默认选项安装即可。

注意:GNS3 不支持中文目录名、文件名,所以一定要将 GNS3 所有工作目录、相关文件名设置为英文。

A.1.2 配置 GNS3 初始环境

GNS3 安装后需要重新启动操作系统，才能正常运行。

1. GNS3 初始配置窗口

GNS3 启动后会出现图 A-1 所示初始配置提示窗口。该窗口提示要使用 GNS3，需要完成两步操作：第 1 步，配置 GNS3 运行参数；第 2 步，导入网络设备 IOS。单击[1]按钮，进入 GNS3 运行参数配置；单击[2]按钮进入导入网络设备 IOS 操作。

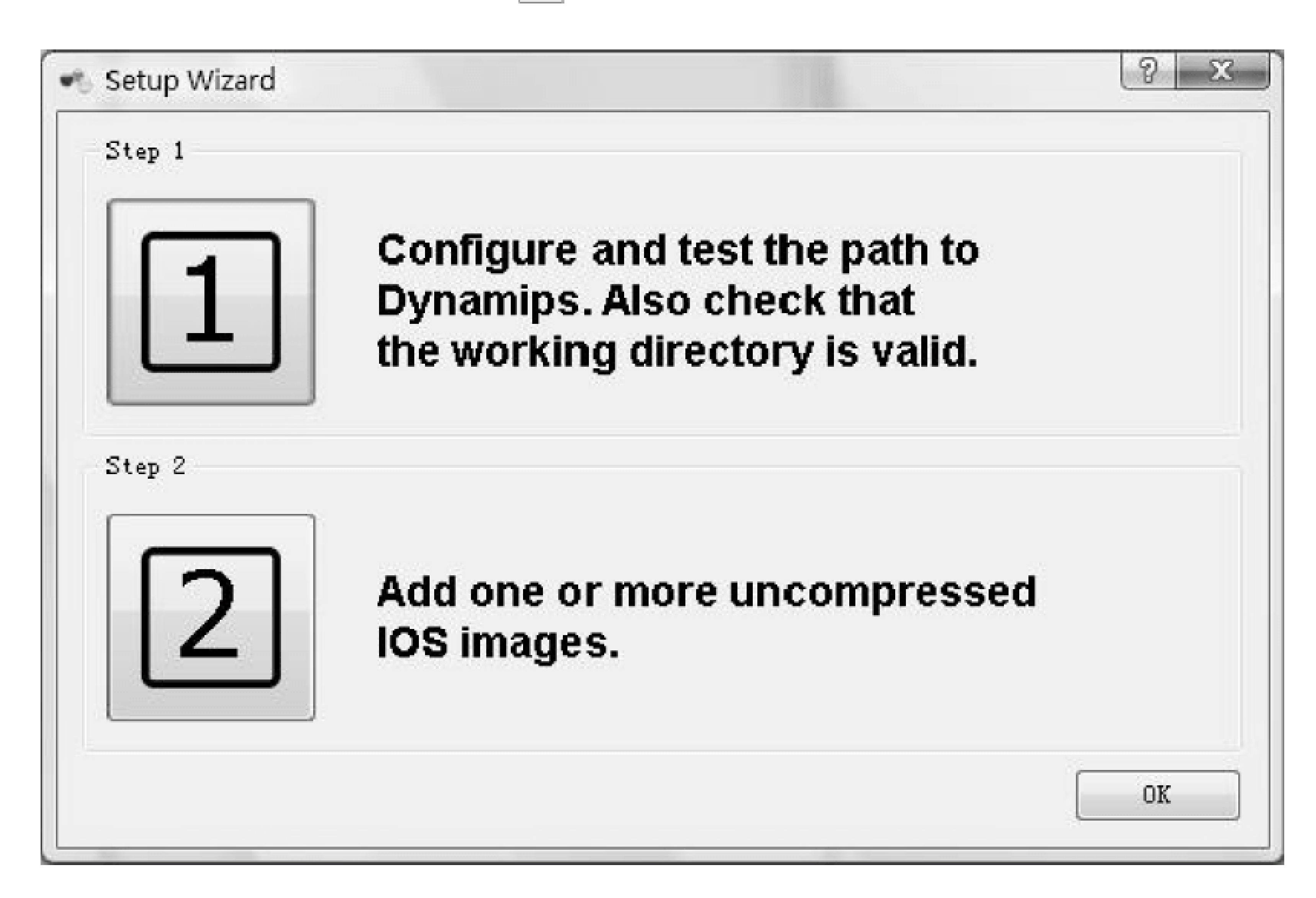


图 A-1 GNS3 初始配置窗口

2. 配置 Dynamips、Pemu 等运行环境参数

如前所述，GNS3 结合了 Dynamips、Pemu 等软件功能，所以在安装 GNS3 后需要配置 Dynamips、Pemu 等运行环境参数。在图 A-1 所示初始配置窗口中单击[1]按钮，或在 GNS3 主窗口中选择 Edit|Preferences 命令，都可以进行 GNS3 运行参数配置。

如图 A-2 所示，GNS3 运行参数配置包括 4 部分：一般配置、Dynamips 配置、Pemu 配置、Capture 配置。

在 GNS3 一般配置中，可以选择软件“语言”为“简体中文”，以便于使用。

另外，需要选择连接到模拟网络设备的终端程序。在 GNS3 首选项窗口中，选择窗口左边列表框中的“一般”选项，在右边“终端命令”文本框中输入 C:\Program Files\Putty\putty.exe -telnet %h %p，让 GNS3 模拟器调用 Putty 软件访问虚拟网络设备，从而可以在终端窗口中对虚拟网络设备进行配置。当然，Putty 软件需要提前安装好。

在 Pemu 配置中，需要为 Cisco PIX 防火墙配置默认 IOS 映像文件、序列号和 KEY，如图 A-3 所示。

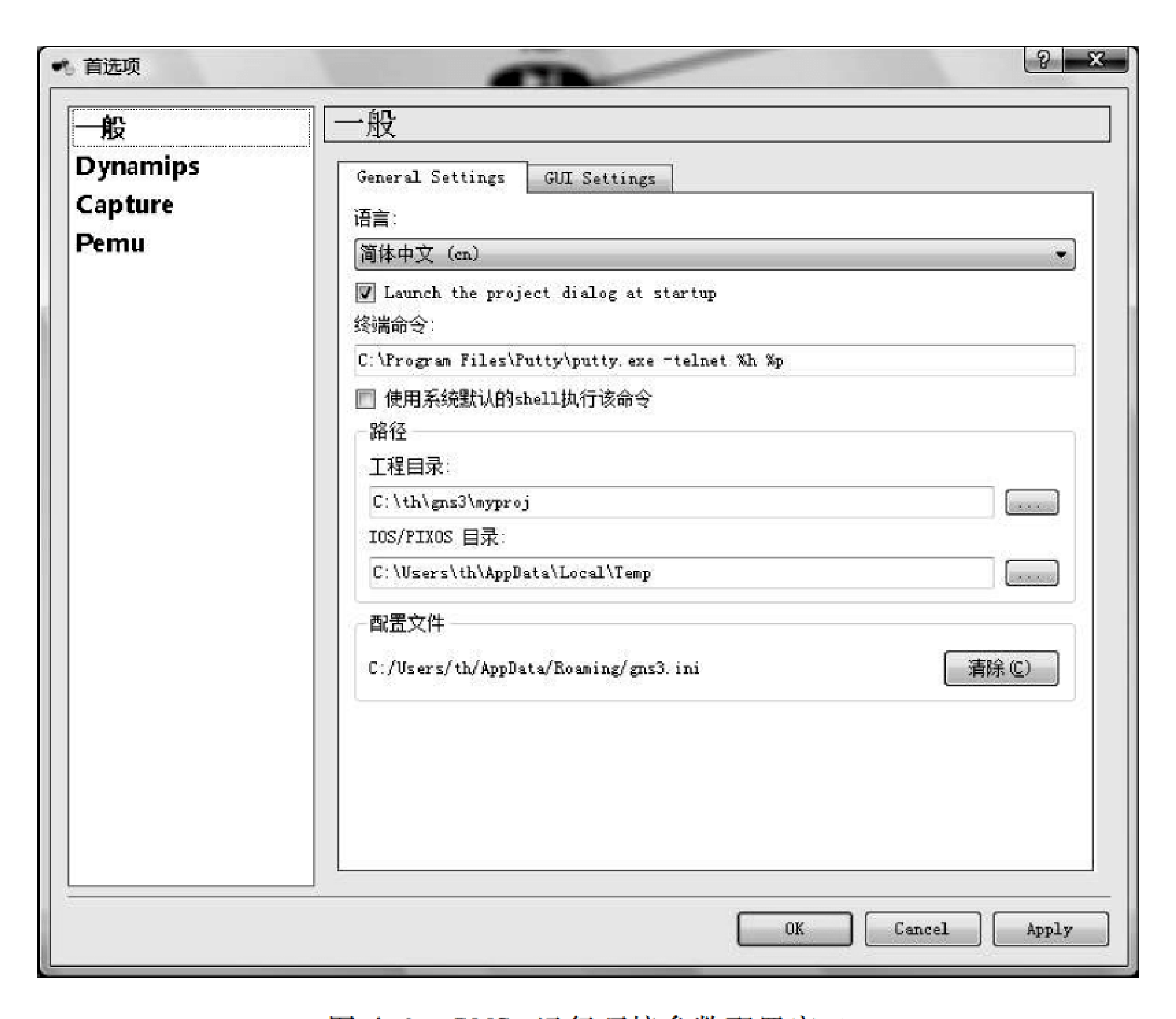


图 A-2 GNS3 运行环境参数配置窗口

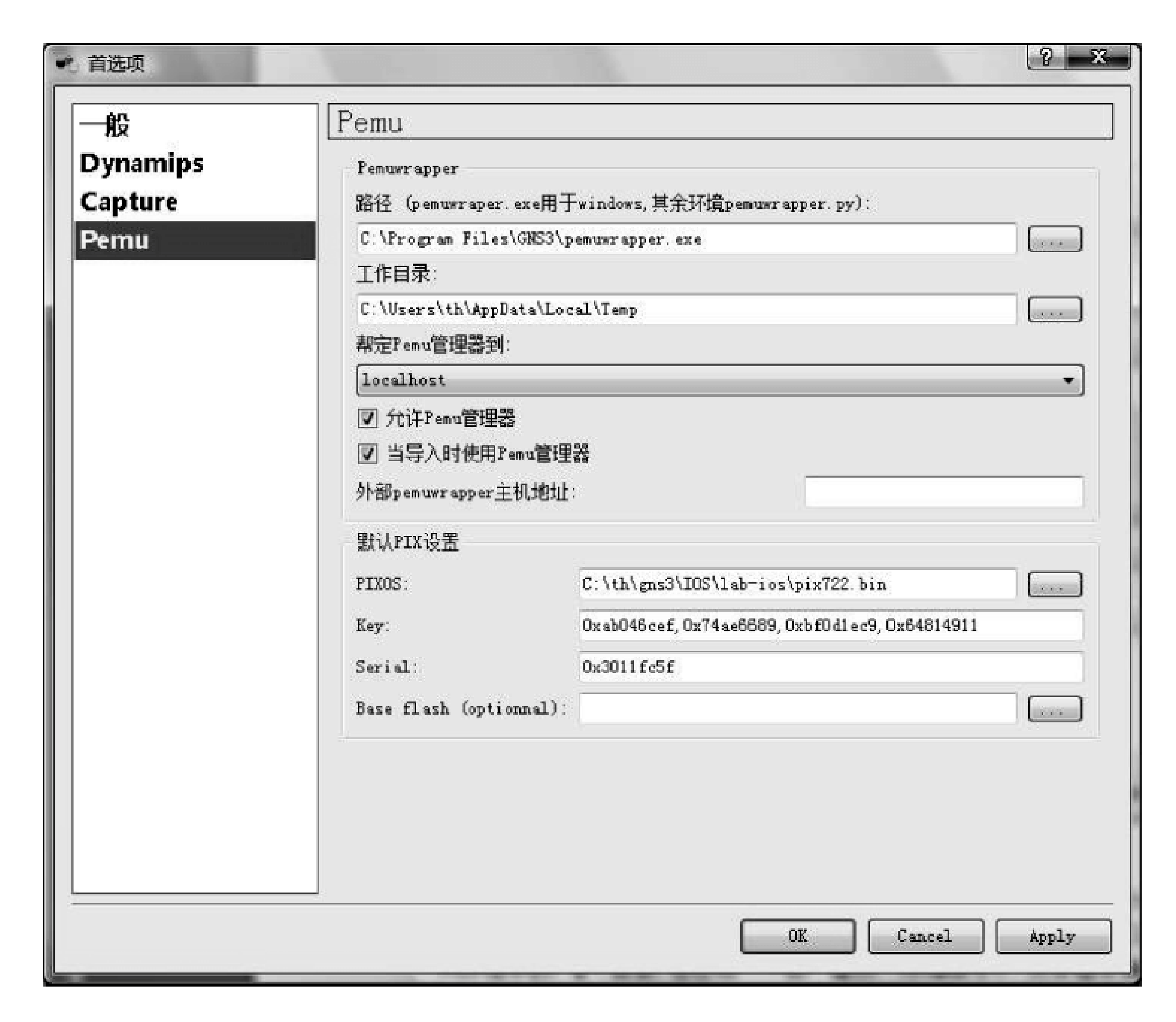


图 A-3 Pemu 运行环境配置窗口

Dynamips 和 Capture 运行环境可以使用默认配置，不用更改。

3. 添加各网络设备 IOS 映像文件

在 GNS3 初始窗口中，单击 2 按钮，或者选择“编辑”|“IOS 和 Hypervisors”命令，都可以打开图 A-4 所示“IOS 和 Hypervisors”窗口，为实验模拟的网络设备导入所需的 IOS 映像文件。

图 A-4　导入 IOS 映像文件窗口

在图 A-4 中的“平台”下拉列表框中，选择需要配置的设备系列号。在“型号”下拉列表框中，选择需要配置的设备型号。单击“IOS 文件”文本框右边的 ... 按钮，找到并选中相应的 IOS 映像文件，单击“打开”按钮确定返回，为所选设备配置 IOS 映像文件。

单击窗口左下方的 保存(S) 按钮，保存配置。此时在窗口上方的 IOS 列表框中会出现所配置的 IOS 映像文件。

A.2　使用 GNS3 模拟网络设备进行实验

使用 GNS3 模拟网络设备的操作非常简单。

在图 A-5 所示主窗口中，用鼠标拖动左边的网络设备图标到中间窗口，然后右击网络设备，在弹出的快捷菜单中选择 开始命令，启动设备。

单击 GNS3 窗口快捷栏上的 按钮，在弹出窗口中选择连接线缆类型，如图 A-6 所示。此时 按钮的图标变为 ，鼠标变为十字形。

用鼠标分别单击要连接的两个网络设备，可以将网络设备连接起来。

单击图 A-5 所示 GNS3 主窗口中的 按钮，打开网络设备终端窗口，即可对网络设备进行配置。

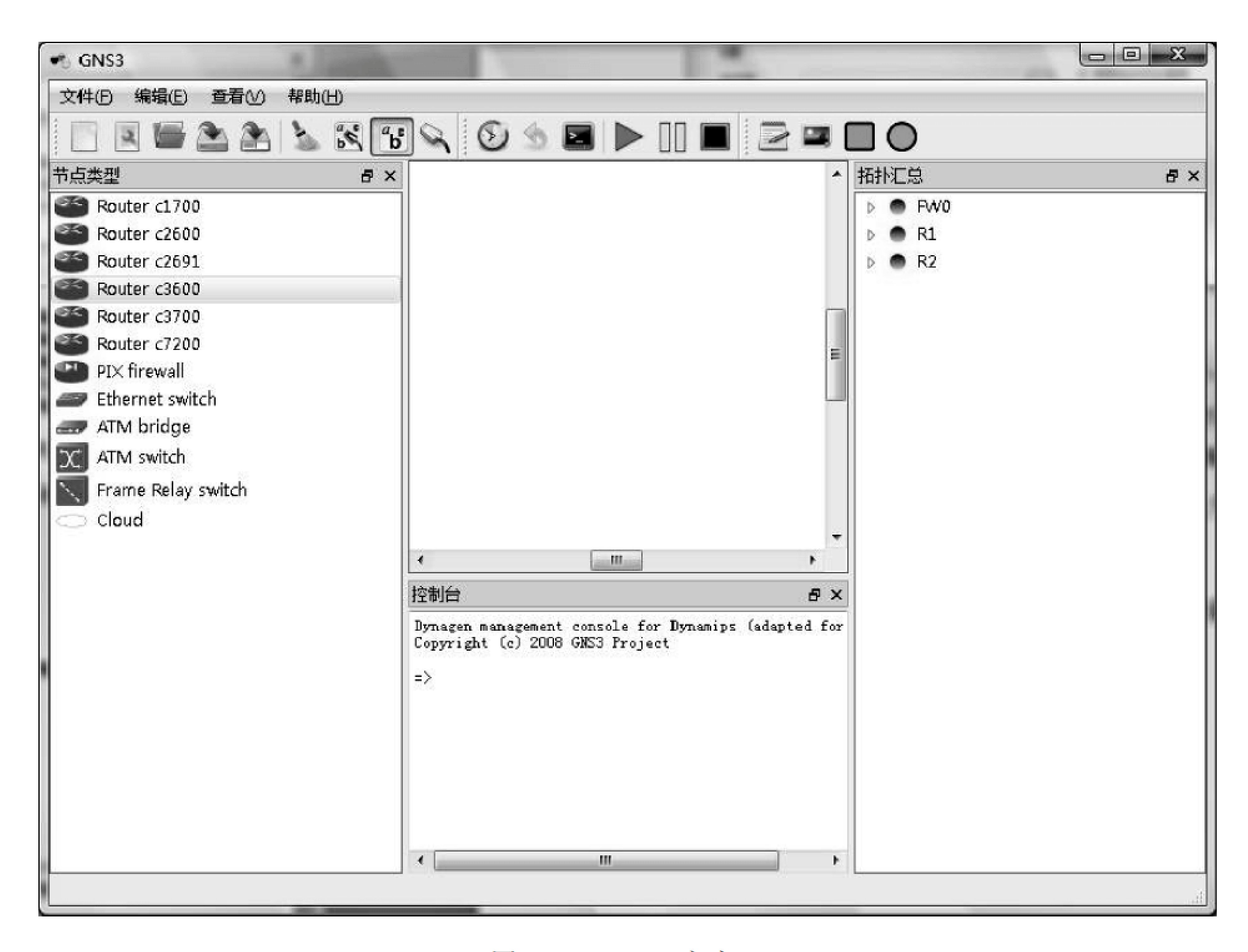


图 A-5 GNS3 主窗口



图 A-6 连接线缆类型菜单

参 考 文 献

[1] (美)Antoon W. Rufi. 网络技术学院教程　网络安全(第一、二学期). 北京邮电大学,思科网络技术学院译. 北京:人民邮电出版社,2008
[2] 蒋建春,邓健. 计算机网络管理理论与实践教程. 北京:北京邮电大学出版社,2008
[3] (美)弗鲁姆,西瓦萨布拉玛尼安,弗拉姆. CCNP 学习指南　组建 Cisco 多层交换网络(BCMSN). 第 4 版. 刘大伟,张芳译. 北京:人民邮电出版社,2007
[4] (美)海吉. 网络安全技术与解决方案. 罗进文等译. 北京:人民邮电出版社,2009
[5] (美)贝塔什. CCSP 自学指南　Cisco 安全 PIX 防火墙(CSPFA). 第 2 版. 孙国冉,王艳奇译. 北京:人民邮电出版社,2005
[6] (美)克莱姆. 网络管理技术构架. 詹文军,杜晓峰,刘玉鹏译. 北京:人民邮电出版社,2008
[7] (美)迪尔. Cisco 路由器防火墙安全. 陈克忠译. 北京:人民邮电出版社,2006